DEPARTMENT OF THE NAVY (DON) DATA MANAGEMENT AND INTEROPERABILITY (DMI) IMPLEMENTATION PLANNING GUIDE

DON CIO Board of Representatives
DMI Integrated Product Team
November 2000

EXECUTIVE SUMMARY

There are both Congressional and Operational mandates for Data Management and Interoperability (DMI). The Clinger-Cohen Act holds government executives and their agencies accountable for delivering systems that produce mission-related results. Other Congressional legislation stresses interoperability, architectures, and system registration as a means to accomplish the objectives stated in the Clinger-Cohen Act. On the operational side, Joint Vision 2010 assumes Information Superiority and Joint Vision 2020 stresses interoperability and decision support. Data are the basic elements of information. Well-structured and defined data is essential to the decision process. Lack of data interoperability negatively impacts speed of command.

DMI is more a management than a technical challenge. Recognizing that budgets and those persons/agencies with control over the budget are key to success in almost any program, the DMI aligns the key data management roles to Resource Sponsors and to dedicated Functional Data Managers who work with system developers. The DMI Integrated Product Team (IPT) recognizes that DMI will be successful only if it is integrated into the requirements, PPBS and acquisition processes and provides a value added over the current way of acquiring and maintaining data.

This Implementation Planning Guide (IPG) is intended to provide a framework and foundation for DON DMI implementation in a rapid and consistent manner. DMI is key to a number of interrelated ongoing strategic initiatives including NMCI, IT-21, Webification and the ERP (Enterprise Resource Planning) Pilots.

The DMI will:

- Provide the infrastructure and management oversight for implementation of the Clinger-Cohen Act and related mandates
- Provide a process for improved operational effectiveness, return on investment, and reduced data costs
- Provide a process to achieve domain and enterprise-level interoperability to support JV2010 and JV2020 goals of information dominance
- Support data quality through the designation of Authoritative Data Sources
- Provide a process to support the capital planning process and IT assessment
- Establish training requirements for IT workforce

The DMI vision is to have global, affordable, and timely access to shared, reliable, and secure data that enables maritime information superiority by 2005. Senior leadership commitment is essential to achieve this vision.

FOREWORD

The Department of the Navy Implementation Planning Guide represents the work of the DON CIO Board of Representatives-chartered Data Management and Interoperability Integrated Product Team (DMI IPT).

The Office of the DON CIO appreciates the dedicated commitment of resources, time and superb talent by all participating organizations.

The DMI IPT met over a period of eleven months in the following locations:

NPGS, Monterey, CA	11/7/99	* Vienna, VA	6/19/00
Dam Neck, VA	12/13/99	* Vienna, VA	7/17/00
Washington, DC	1/24/00	* Vienna, VA	8/21/00
San Diego, CA	2/27/00	* San Diego, CA	9/19/00
Pensacola, FL	4/10/00	* Vienna, VA	10/16/00
Everett, WA	5/22/00	* Writing Team Sessions	

The office of the DON CIO would like to thank the following people for their contributions to the Data Management and Interoperability effort:

*	Melanie Winters	CINCPACFLT	IPT Leader
*	George Endicott	SPAWAR 05	Management Subteam Lead
*	Mary Hutton	CNO N1	Architecture Subteam Lead
*	Dan Walters	FIWC	Metadata Repository Subteam Lead

	Pat Ashton	NAVSUP
	Kevin Beckwith, ITC	NAVPERS 07
*	Becky Bennett	NAVFAC
*	Ralph Bishop	FIWC/GRCI
*	Bob Buckley	PEO (IT) ITC
*	Mary Chervenic	CNO N6 C/K
	Paul Cox	COMNAVSPACECOM
	LCDR Susan Davis	CNO N7
*	Bob Dickie	COMNAVSECGRU N6
*	Becky Ferris	Coastal Systems Station
	Joe Garner	NSWC Carderock
	Robert Hayes	COMNAVSECGRU N6
*	Terry Howell	SPAWAR
*	Mike Jennings	SPAWAR (Intelisis)
	David Jones	NSGA Northwest
	Edward Kirkpatrick	CNO N4T
	Enrique Kortright	PEO (IT) ITC
	Jerry Lattig	NAVSUP
	Sid Mills	SEO/MP
	Bill Moran (OSC(SW))	CINCLANTFLT N66
	Tom Nabors	COMNAVMETOCCOM
*	Giao Nguyen	SPAWAR
	Lo Retta Parrish (ITC)	NAVPERS 073N
	Susan Peed	USMC
	Carol Pepper	CNET
	Neal Pollock	PEO (IT)

	Lynda Race, LCDR	NMIMC
	Cindy Randall	NAVAIR
	Mike Rice	NAVSEA 53
	Jim Seevers, CTIC	COMNAVSECGRU N6
	Bernadette Semple, LCDR	CNO N6 C/K
	Olen Sisson	DON OMIT
	Anne Slingerland	MARCORSYSCOM
	Larry Stack, CAPT	CNO N6 C/K
	Randy Summers	FIWC
	Virginia Thiebaud	PACNORWEST
	Barbara Vaughn	NAVAIR 4.0E
	Faye Watson	COMNAVSPACECOM
	Dennis Wells, LCDR	CNO N7
	Mary Whitfield	COMNAVRESFOR
	Joyce Wineland	ONI
*	Brian Wilczynski	DON CIO
	Scott Badger	DON CIO (BAH)
*	Gregg Hanold	DON CIO (SEICORP)
*	Bob Helsel	DON CIO (RDH Enterprises)
*	Dave Howes	DON CIO (Silver Bullet Solutions)
*	Robert Lewis	DON CIO (BAH)
	Dave McDaniel	DON CIO (Silver Bullet Solutions)
	Jim McKee	DON CIO (GRCI/AT&T)
*	Greg Michaels	DON CIO (GRCI/AT&T)

* Member of Implementation Planning Guide Writing Team

TABLE OF CONTENTS

Section **Page**

TABLE OF CONTENTS

Section **Page**

TABLE OF CONTENTS (Cont'd)

Section **Page**

TABLE OF CONTENTS (Cont'd)

Section **Page**

LIST OF EXHIBITS

1. DMI IMPLEMENTATION REQUIREMENTS

There are both Congressional and Operational mandates for Data Management and Interoperability (DMI).

In 1996, Congress passed the Clinger-Cohen Act which establishes Chief Information Office (CIO) responsibilities for ensuring that investments in Information Technology (IT) improve performance by supporting mission statements, long-term goals and objectives, and annual performance plans that are developed under the Government Management Reform Act (GMRA) of 1994. In short, under the Clinger-Cohen Act government executives and their agencies are accountable for delivering systems that produce mission-related results. Since then, Congress has passed additional legislation, referencing the Clinger-Cohen Act, which stress interoperability, architectures, and system registration as a means to accomplish the objectives stated in the Clinger-Cohen Act.

On the operational side, the Joint Chiefs have issued Joint Vision 2010 which assumes Information Superiority in order to support new operational concepts, and Joint Vision 2020 which stresses interoperability and decision support. This follows a review of Gulf War lessons learned, lethality of new weapons, the threat of terrorism, and reduced budgets. Two overriding conclusions are: (1) U.S. success in future battle and contingency operations hinges on an information advantage, and (2) a key component to interoperability is the development and implementation of a strong architecture and standards management program.

Accordingly, the DON CIO and an Integrated Product Team (IPT) developed a DON Data Management and Interoperability Strategic Plan and SECNAVINST to implement a DON DMI infrastructure. Exhibit 1, DON Data Management and Interoperability, shows the scope of DMI.

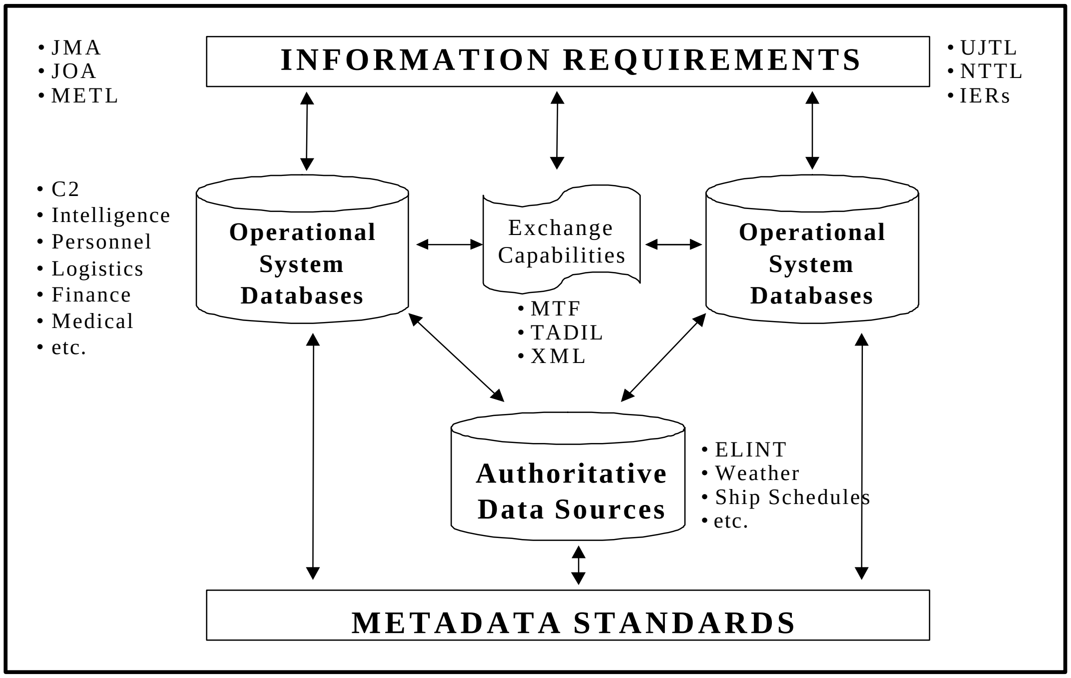


Exhibit 1. DON Data Management and Interoperability

The IPT developed this DMI Implementation Planning Guide to provide the means of implementing the Mission and Vision in the Strategic Plan in accordance with the policy in the SECNAVINST. The intended audience for this document includes senior Information Management/Information Technology (IM/IT) managers, CNO/CMC Resource and Program Sponsors, Program Executive Officers (PEO) and Program Managers (PM) and data management professionals at all levels. The scope of this document covers the development of data architectures and associated data standards for both warfare and warfare support areas.

This document is divided into three sections:

- Section 1, DMI Requirements, addresses the Congressional and operational mandates and DON approach for putting in place an infrastructure to satisfy them. It is written from the standpoint of "what" DMI is and "why" it is needed.
- Section 2, DMI Concept of Operations, provides the "how" the infrastructure will accomplish its mission.
- Section 3, Plan of Actions and Milestones (POA&M), addresses the "who" has responsibility for DMI actions and "when" the actions are to be achieved.

1.1. Congressional, DOD, and Operational Requirements for DMI

There are numerous directives and other governing documents that affect DMI. The principal documents are identified below.

a. Government Performance and Results Act (GPRA) of 1993 requires the establishment of strategic planning and performance measurement in the Federal Government. OMB has mandated that strategic plans cover six-years and be updated every three years.

b. Title 40, United States Code, Chapter 25, as amended (Codifies Public Law 104-106, "National Defense Authorization Act for Fiscal Year 1996," Division E (Clinger-Cohen Act), February 10, 1996). The Clinger-Cohen Act specifies Chief Information Officer (CIO) responsibilities for Information Technology (IT) and mandates improvement in day-to-day mission processes and proper use of IT to support those improvements. The Clinger-Cohen Act provides the following definitions:

- **Information Technology.** Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term "equipment" in this definition means equipment used by a Component directly, or used by a contractor under a contract with the Component, which requires the use of such equipment, or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "IT" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "IT" includes National Security Systems. (40 USC 1401 and Reference (a), Sec 5002)

- **National Security System.** Any telecommunications or information system operated by the United States Government, the function, operation, or use of which: (a) involves intelligence activities; (b) involves cryptologic activities related to national security; (c) involves command and control of military forces; (d) involves equipment that is an integral part of a weapon or weapons system; or (e) subject to limitation below, is critical to the direct fulfillment of military or intelligence missions. Limitation—Item (e) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

c. Title 10, United States Code, Chapter 131, Section 2223 (Codifies Public Law 105-261, "National Defense Authorization Act FY99," Section 331, October 17, 1998). Public Law 105-261 states the Chief Information Officer of a military department, with respect to the military department concerned, shall: (1) review budget requests for all information technology and national security systems; (2) ensure that information technology and national security systems are in compliance with standards of the Government and the Department of Defense; (3) ensure that information technology and national security systems are interoperable with other relevant information technology and national security systems of the Government and the Department of Defense; and (4) coordinate with the Joint Staff with respect to information technology and national security systems.

d. FY 2001, Defense Appropriation Act, Section 8102 states that none of the funds appropriated in this Act may be used for a mission critical or mission essential information technology system (including a system funded by the defense working capital fund) that is not registered with the Chief Information Officer of the Department of Defense. A major automated information system may not receive Milestone I approval, Milestone II approval, or Milestone III approval within the Department of Defense until the Chief Information Officer certifies, with respect to that milestone, that the system is being developed in accordance with the Clinger-Cohen Act. The Chief Information Officer may require additional certifications, as appropriate, with respect to any such system. Reporting is in the form of a database and the reporting structure of the information will need to enable sharing of registration data in the DoD.

e. OMB Circular A-130, Management of Federal Information Resources, currently under revision requires agencies to create an Enterprise Architecture together with a supporting Technical Reference Model and Standards Profile.

f. DOD Directive 4630.5 under revision "Information Interoperability and Supportability" implements Clinger-Cohen Act and directs an outcome–based approach to ensure interoperability of Information Technology and National Security Systems (NSS) throughout the DOD. It establishes that requirements for information interoperability be characterized in a family of systems (FoS) or system of systems (SoS) joint area mission context for all IT and NSS capabilities. The following definitions apply:

- **Family of Systems**. A set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capabilities. The mix of systems can be tailored to provide desired capabilities dependent on the situation.

- **System of Systems**. A set or arrangement of systems that are related or connected to provide a given capability. The loss of any part of the system will degrade the performance or capabilities of the whole.

g. DOD Directive 8320.1 of 26 Sep 91, "DOD Data Administration" requires that DOD data management be implemented to support operations and decision making with data that meets the need in terms of availability, accuracy, timeliness and quality. It also cites the need to structure the information to enable horizontal, as well as vertical, sharing of data in the DOD.

h. DOD 8320.1-M-1 of Apr 1998, "Data Standardization Procedures" prescribes procedures for the development, approval, and maintenance of DOD data standards necessary to support the policies of DOD Data Administration as established by DOD Directive 8320.1.

i. DOD Architecture Framework, Version 2.1 implements OMB A-130 in DOD using C41SR Architecture Framework, including C41SR Architecture Data Model (CADM) as a foundation.

j. Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS), Version 4.0 of 25 Oct 1999 describes the technical requirements for using the Defense Information Infrastructure (DII) Common Operating Environment (COE) to build and integrate systems. It specifies levels of DII compliance that are tied to levels of interoperability for applications, and database segments which are being developed as part of the Shared Data Engineering (SHADE) effort.

k. Joint Vision 2020, the capstone joint warfighting strategic plan, recognizes information superiority as the foundation for new joint doctrine and concepts. It defines information superiority in terms of continuing emphasis on interoperability as a critical enabler for harvesting the benefits of the ongoing Revolutions in Military and Business Affairs.

l. CJCSI 6212.01A of 30 June 1995, "Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence Systems states all C4I systems, and computer resources associated with weapon systems, developed for use by or in support of US forces are defined to be for use in joint operations and must be certified as "interoperable" with systems with which they have a requirement to exchange information. Interoperability requires that systems are interoperable vertically and horizontally to the degree specified by the warfighter and necessary to ensure timely, efficient, and survivable C4I functions at all force levels."

m. SECNAVINST 5239 (Draft), Department of the Navy Information Assurance (IA) Policy, includes IA as a critical component of the IT life cycle management process and states all IT systems under DON authority must be IA certified and accredited for use.

The Congressional requirements are being implemented within DOD, within the context of "Information Superiority" for a U.S. military strategy. In a 15 July 1999 memo, ASD C3I stated, "Information Superiority, as defined in JV2010, has lead to a continuing emphasis on interoperability as a critical enabler for harvesting the benefits of the Revolutions in Military and Business Affairs. No longer is the importance of interoperability among myriad systems, applications and data that compose the DOD Information Technology, a subject for debate.

1.1.1. Assessments

The Clinger-Cohen Act is part of a major legislative effort to improve government. The Act imposes a number of requirements that seek to ensure that appropriate information is considered and assessed before IT acquisition decisions are made. Specifically, among the requirements is the need to ensure that all IT requirements can be linked to mission, and that measures of performance are established to document return on investment. The Clinger-Cohen Act requires agencies to design and implement a process that will maximize value and assess and manage the risk of IT investments. This assessment of relevant information is to continue after the system is implemented – agencies are required to establish performance measures and evaluate the results and benefits of IT investments. The requirement for an integrated IT Capital Planning and Investment Control model is a key provision of the Clinger-Cohen Act. This requirement has resulted in changes to the DoD capital planning investment control process - the Planning, Programming and Budgeting System (PPBS).

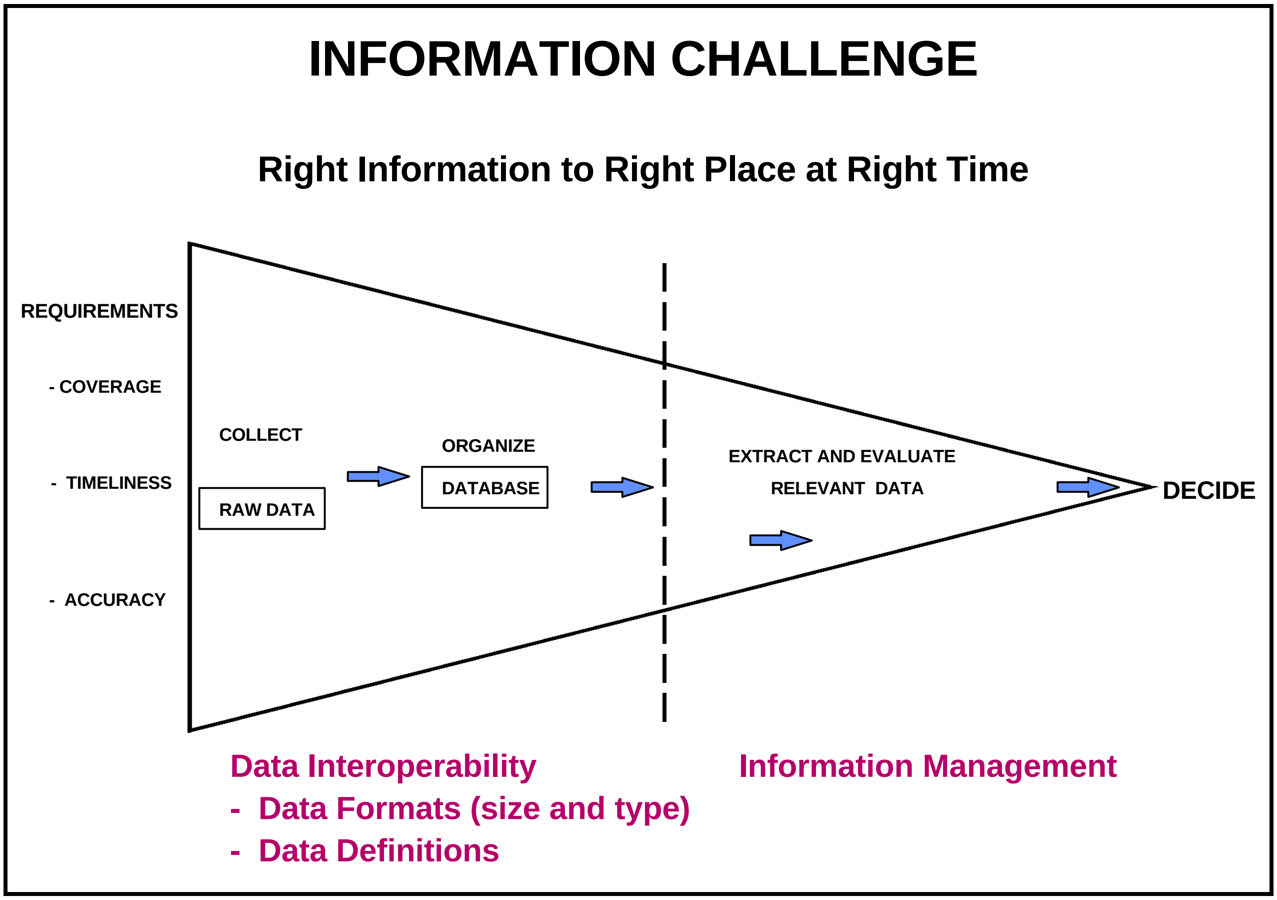
Developing useful and appropriate performance measures is key to satisfying the requirements of the Clinger-Cohen Act. Performance measures should:

- Provide a linkage to DoD’s Strategic Plan, Budget Plan and other planning processes.
- Clarify objectives and provide direction.
- Provide a baseline to obtain feedback and recognize performance.
- Help gauge results of IT initiatives and determine whether to continue, modify, or cancel an ongoing program, project, or acquisition.

1.1.2. Joint Systems Interoperability at the Data Level

Information systems interoperability is the measured ability of systems to exchange information at the level(s) of sophistication required to support critical functional and mission operations, and at higher levels of sophistication to assure flexibility to engage in more demanding operations that cannot be predicted nor planned in advance.

Exhibit 2, The DMI Operational Challenge, shows that well structured and defined data is essential to the decision process. Lack of data interoperability impacts speed of command.



INFORMATION CHALLENGE

Right Information to Right Place at Right Time

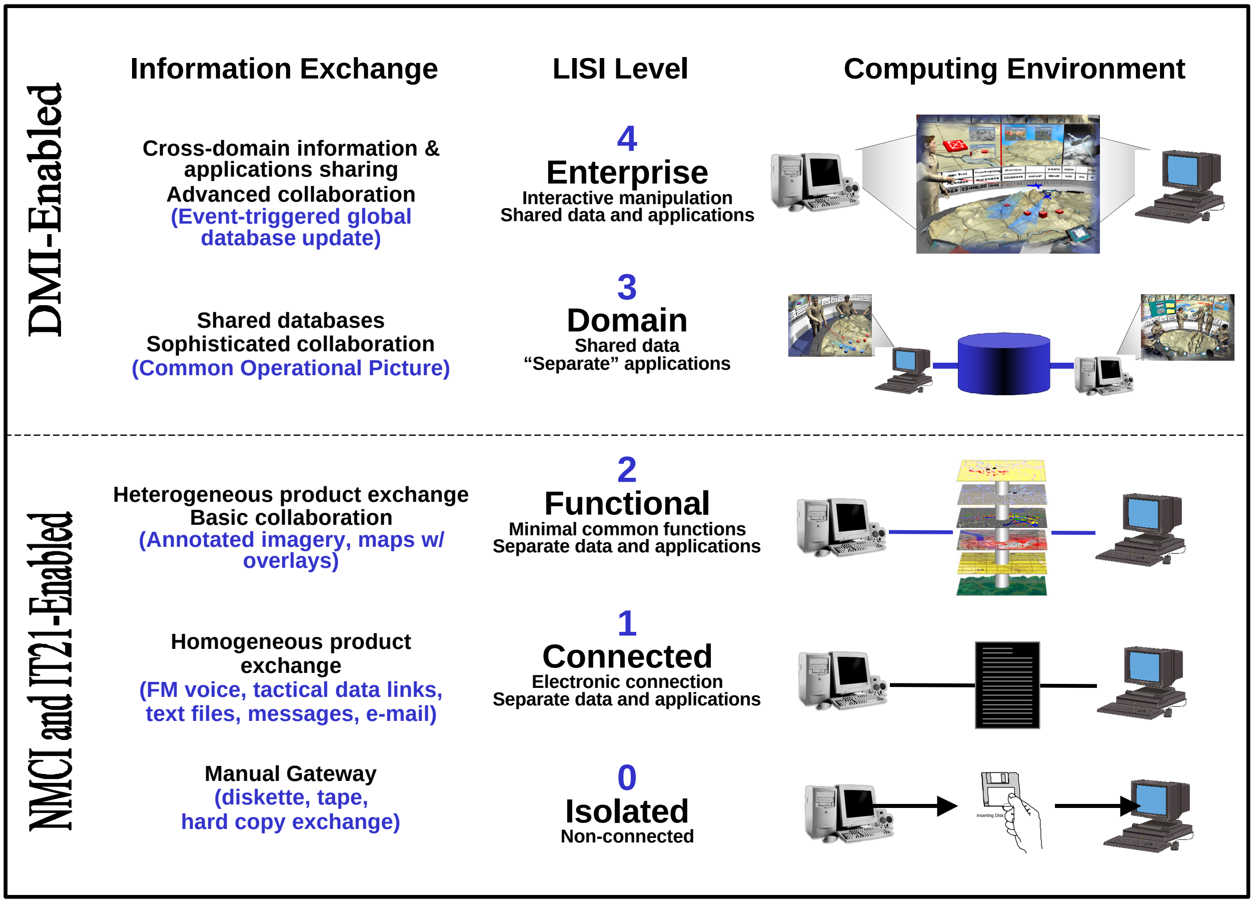
Data Interoperability
- Data Formats (size and type)
- Data Definitions

Information Management

Exhibit 2. The DMI Operational Challenge

Exhibit 3, The DMI Technical Requirement, shows the technical challenge and progression from simple hardware and software connectivity through shared data to full systems interoperability across the Enterprise. The ability of systems to interoperate at any specific level of sophistication or "maturity" is determined by three essential conditions:

- The sufficiency of the systems' inherent core capabilities, i.e., the policies and procedures that govern the systems' implementations and use, the system applications and services, the systems' infrastructure interface capabilities, and the systems' data characteristics.
- The compatibility of the systems' implementations of these core capabilities.
- The adequacy of the prevailing infrastructure within which the systems may interoperate.

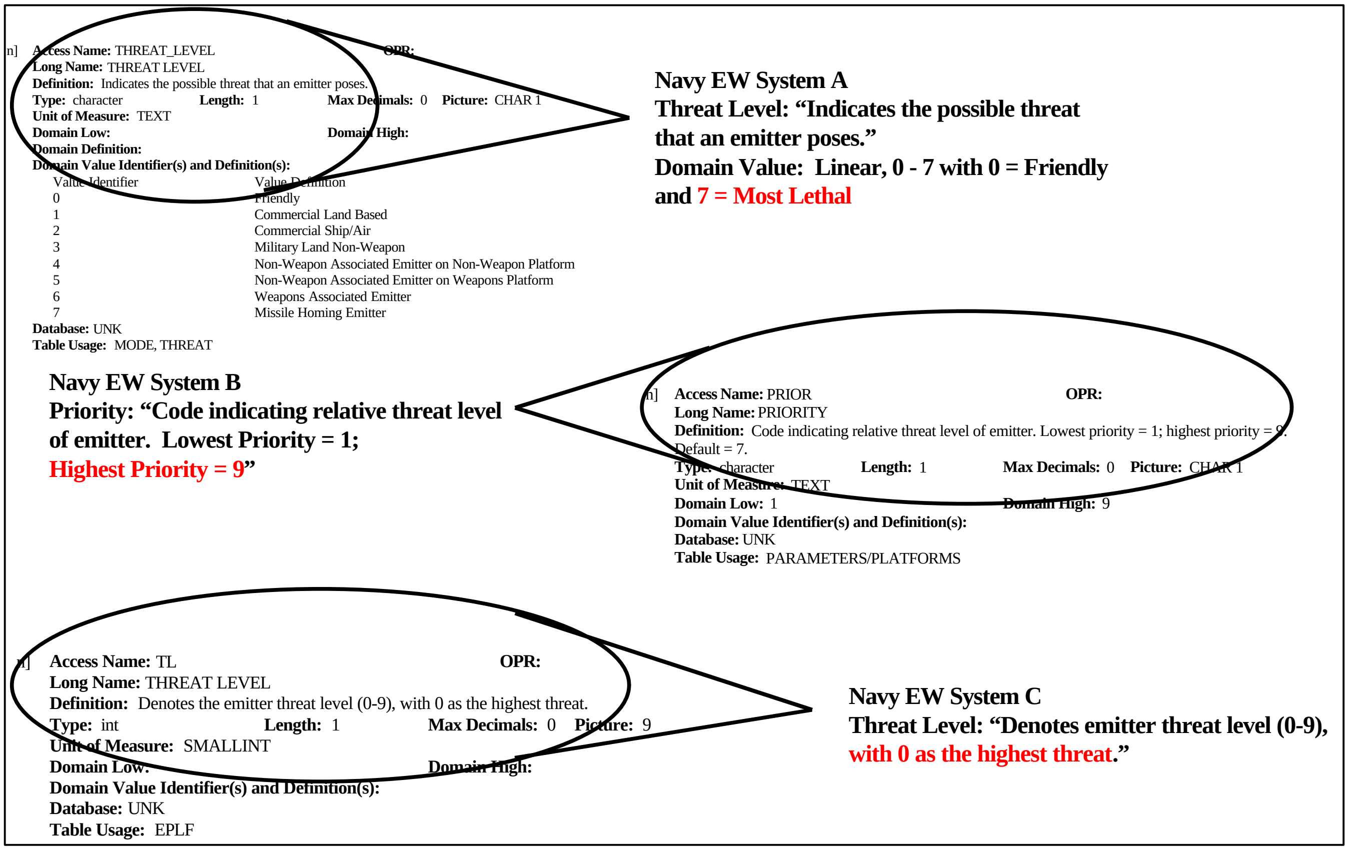


	Information Exchange	LISI Level	Computing Environment
DMI-Enabled	Cross-domain information & applications sharing Advanced collaboration (Event-triggered global database update)	4 Enterprise Interactive manipulation Shared data and applications	
	Shared databases Sophisticated collaboration (Common Operational Picture)	3 Domain Shared data "Separate" applications	
NMCI and IT21-Enabled	Heterogeneous product exchange Basic collaboration (Annotated imagery, maps w/ overlays)	2 Functional Minimal common functions Separate data and applications	
	Homogeneous product exchange (FM voice, tactical data links, text files, messages, e-mail)	1 Connected Electronic connection Separate data and applications	
	Manual Gateway (diskette, tape, hard copy exchange)	0 Isolated Non-connected	

Exhibit 3. The DMI Technical Requirement

In order to achieve Information Superiority, the Navy/Marine Corps Intranet and IT21 need to reach levels 3 and 4 of the Levels of Information System Interoperability (LISI) maturity model. Systems interoperability at the data level is dependent upon harmonizing metadata (data about data) and software applications with their associated infrastructure.

Metadata is information describing the characteristics of data; data or information about data; descriptive information about an organization's data, data activities, systems, and holdings. It is about packaging and definitions. Exhibit 4, System Data Inconsistency – Navy Example, shows different ways of portraying threat levels in three Navy Electronic Warfare (EW) Systems. This data was collected as part of an effort to define "Combat Identification: in data terms. The effort was sponsored by NAVSEA and executed by the Data Requirements Working Group (DRWG) under the technical leadership provided by the Fleet Information Warfare Center (FIWC). To date, metadata on 45 EW and combat systems has been collected, and it becomes obvious that each program did not have visibility into the data engineering details of the other systems.



n] **Access Name:** THREAT_LEVEL **OPR:**
Long Name: THREAT LEVEL
Definition: Indicates the possible threat that an emitter poses.
Type: character **Length:** 1 **Max Decimals:** 0 **Picture:** CHAR 1
Unit of Measure: TEXT
Domain Low: **Domain High:**
Domain Definition:
Domain Value Identifier(s) and Definition(s):

Value Identifier	Value Definition
0	Friendly
1	Commercial Land Based
2	Commercial Ship/Air
3	Military Land Non-Weapon
4	Non-Weapon Associated Emitter on Non-Weapon Platform
5	Non-Weapon Associated Emitter on Weapons Platform
6	Weapons Associated Emitter
7	Missile Homing Emitter

Database: UNK
Table Usage: MODE, THREAT

Navy EW System A
Threat Level: "Indicates the possible threat that an emitter poses."
Domain Value: Linear, 0 - 7 with 0 = Friendly and 7 = Most Lethal

Navy EW System B
Priority: "Code indicating relative threat level of emitter. Lowest Priority = 1; Highest Priority = 9"

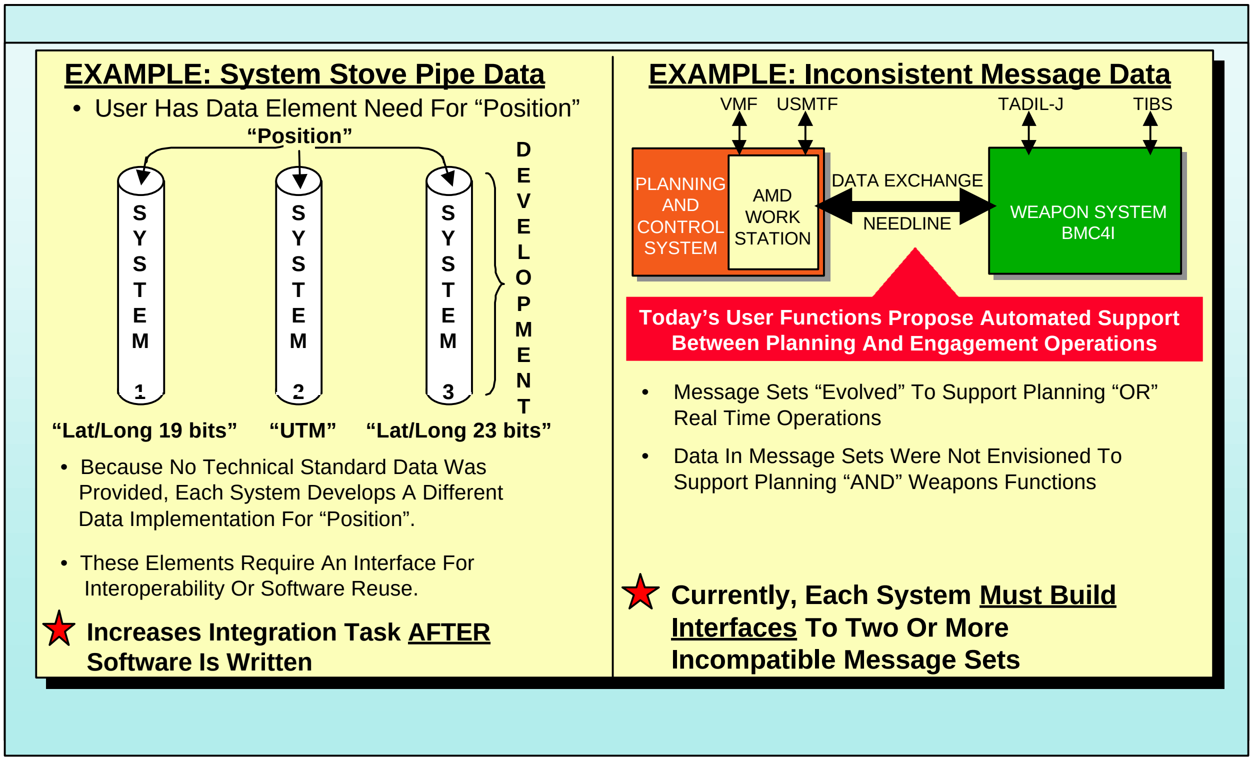
n] **Access Name:** PRIOR **OPR:**
Long Name: PRIORITY
Definition: Code indicating relative threat level of emitter. Lowest priority = 1; highest priority = 9. Default = 7.
Type: character **Length:** 1 **Max Decimals:** 0 **Picture:** CHAR 1
Unit of Measure: TEXT
Domain Low: 1 **Domain High:** 9
Domain Value Identifier(s) and Definition(s):
Database: UNK
Table Usage: PARAMETERS/PLATFORMS

n] **Access Name:** TL **OPR:**
Long Name: THREAT LEVEL
Definition: Denotes the emitter threat level (0-9), with 0 as the highest threat.
Type: int **Length:** 1 **Max Decimals:** 0 **Picture:** 9
Unit of Measure: SMALLINT
Domain Low: **Domain High:**
Domain Value Identifier(s) and Definition(s):
Database: UNK
Table Usage: EPLF

Navy EW System C
Threat Level: "Denotes emitter threat level (0-9), with 0 as the highest threat."

Exhibit 4. System Data Inconsistency – Navy Example

Exhibit 5, System Data Inconsistency – Army Example, shows the challenge to building a Family of Systems or System of Systems without data standards that are developed within an operational context.



EXAMPLE: System Stove Pipe Data

- User Has Data Element Need For "Position"

- Because No Technical Standard Data Was Provided, Each System Develops A Different Data Implementation For "Position".
- These Elements Require An Interface For Interoperability Or Software Reuse.

★ **Increases Integration Task AFTER Software Is Written**

EXAMPLE: Inconsistent Message Data

Today's User Functions Propose Automated Support Between Planning And Engagement Operations

- Message Sets "Evolved" To Support Planning "OR" Real Time Operations
- Data In Message Sets Were Not Envisioned To Support Planning "AND" Weapons Functions

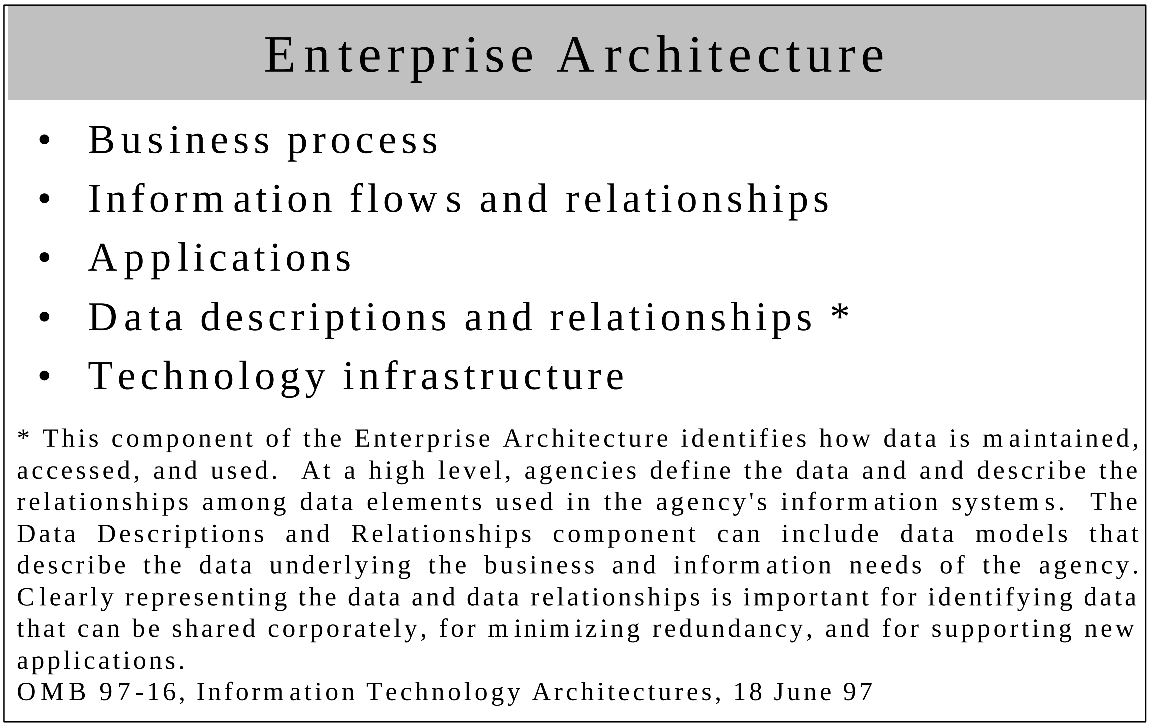
★ **Currently, Each System Must Build Interfaces To Two Or More Incompatible Message Sets**

Exhibit 5. System Data Inconsistency – Army Example

The data inconsistencies shown are not solvable by hardware or software, or new technologies like XML. Middleware can help the problem, but it has limitations, specifically when another system is using different software. The Naval Warfare Tactical Database Flag Steering Group concluded between 1984 – 1990 that interoperability is more a management problem than a technical problem. Contributing to that conclusion was a lack of suitable standardization technologies and methodologies, lack of pragmatic process, few qualified technical personnel, and fewer still high-level managers confronting the issue. That situation is changing.

1.1.3. Architecture and Standards

The Clinger-Cohen Act requires an IT architecture which is identified as a CIO responsibility. Public Law 105-261 states that interoperability will be achieved by synchronizing architectures. OMB Circular A-130 implements Clinger-Cohen. Exhibit 6, Mandatory OMB Circular A-130 Architecture Components, shows the minimum components of an Enterprise Architecture.



Enterprise Architecture

- Business process
- Information flows and relationships
- Applications
- Data descriptions and relationships *
- Technology infrastructure

* This component of the Enterprise Architecture identifies how data is maintained, accessed, and used. At a high level, agencies define the data and and describe the relationships among data elements used in the agency's information systems. The Data Descriptions and Relationships component can include data models that describe the data underlying the business and information needs of the agency. Clearly representing the data and data relationships is important for identifying data that can be shared corporately, for minimizing redundancy, and for supporting new applications.

OMB 97-16, Information Technology Architectures, 18 June 97

Exhibit 6. Mandatory OMB Circular A-130 Architecture Components

DoD is implementing A-130 requirements through the DoD Architecture Framework that is being developed using the C4ISR Architecture Framework as its foundation. Exhibit 7, Mandatory and Supporting DoD Architecture Framework Products, Version 2.1 shows the mandatory and supporting operational, systems, and technical products required for systems development. In addition to the mandatory DoD products, DON DMI also will require systems provide an OV-7, Logical Data Model, and an SV-11, Physical Data Model as well as a Conceptual Data Model. These products are defined in Section 1.2.5.

Applicable Architecture View	Product Reference	Architecture Product	Mandatory Joint or Supporting Specific-Purpose	General Description
All Views (Context)	AV-1	***Overview and Summary Information***	**Mandatory**	Scope, purpose, intended users, environment depicted,analytical findings, if applicable
All Views (Terms)	AV-2	***Integrated Dictionary***	**Mandatory**	Definitions of all terms used in all products
All Views (Capabilities))	AV-3	***Capability Maturity Profile***	Supporting	Description of focus areas in terms of incremental capability levels, consistent with a standard capability maturity scale.
Operational	OV-1	***High-level Operational Concept Description***	**Mandatory**	High-level graphical and textual description of operational concept (high-level organizations, missions, geographic configuration, connectivity, etc.)
Operational	OV-2	***Operational Node Connectivity Description***	**Mandatory**	Operational nodes, activities performed at each node, connectivities & information flow between nodes
Operational	OV-3	***Operational Information Exchange Matrix***	**Mandatory**	Information exchanged between nodes and the relevant attributes of that exchange such as media, quality, quantity, and the level of interoperability required.
Operational	OV-4	***Organizational Relationships Chart***	Supporting	Command, control, coordination, other relationships among organizations
Operational	OV-5	***Activity Model***	**Mandatory**	Activities, relationships among activities,inputs and outputs. In addition overlays can show cost, performing nodes, or other pertinent information.
Operational	OV-6a	***Operational Rules Model***	Supporting	One of the three products used to describe operational activity sequence and timing that identifies the business rules that constrain the operation
Operational	OV-6b	***Operational State Transition Description***	Supporting	One of the three products used to describe operational activity sequence and timing that identifies responses of a business process to events
Operational	OV-6c	***Operational Event/Trace Description***	Supporting	One of the three products used to describe operational activity sequence and timing that traces the actions in a scenario or critical sequence of events
Operational	OV-7	***Logical Data Model***	Supporting	Documentation of the data requirements and structural business process rules of the Operational View.
Systems	SV-1	***System Interface Description***	**Mandatory**	Identification of systems and system components and their interfaces, within and between nodes
Systems	SV-2	***Systems Communications Description***	Supporting	Physical nodes and their related communications laydowns
Systems	SV-3	***Systems^2 Matrix***	Supporting	Relationships among systems in a given architecture; can be designed to show relationships of interest, e.g., system-type interfaces, planned vs. existing interfaces, etc.
Systems	SV-4	***Systems Functionality Description***	Supporting	Functions performed by systems and the information flow among system functions
Systems	SV-5	***Operational Activity to System Function Traceability Matrix***	Supporting	Mapping of system functions back to operational activities
Systems	SV-6	***System Data Exchange Matrix***	Supporting	Detailing of data exchanges among system elements, applications and H/W allocated to system elements
Systems	SV-7	***System Performance Parameters Matrix***	Supporting	Performance characteristics of each system(s) hardware and software elements, for the appropriate timeframe(s)
Systems	SV-8	***System Evolution Description***	Supporting	Planned incremental steps toward migrating a suite of systems to a more efficient suite, or toward evolving a current system to a future implementation
Systems	SV-9	***System Technology Forecast***	Supporting	Emerging technologies and software/hardware products that are expected to be available in a given set of timeframes, and that will affect future development of the architecture
Systems	SV-10a	***Systems Rules Model***	Supporting	One of three products used to describe systems activity sequence and timing -- Constraints that are imposed on systems functionality due to some aspect of systems design or implementation
Systems	SV- 10b	***Systems State Transition Description***	Supporting	One of three products used to describe systems activity sequence and timing -- Responses of a system to events
Systems	SV -10c	***Systems Event/Trace Description***	Supporting	One of three products used to describe systems activity sequence and timing -- System-specific refinements of critical sequences of events described in the operational view
Systems	SV-11	***Physical Data Model***	Supporting	Physical implementation of the information of the Logical Data Model, e.g., message formats, file structures, physical schema
Technical	TV-1	***Technical Architecture Profile***	**Mandatory**	Extraction of standards that apply to the given architecture
Technical	TV-2	***Standards Technology Forecast***	Supporting	Description of emerging standards that are expected to apply to the given architecture, within an appropriate set of timeframes

Exhibit 7. Mandatory and Supporting DoD Architecture Framework Products

1.1.4. Systems Registration

The FY 2001, Defense Authorization Act requires the registration of a mission critical or mission essential system as a part of the Milestone approval process for major automated information systems. These systems represent billions of dollars in investment and provide the foundation for establishing an "as is" Enterprise systems data requirements/capabilities baseline. To construct this baseline, it is necessary to address data, data transfer formats, software applications, and supporting infrastructure within a common IT context. It also is necessary to tie architecture and standards to the acquisition process. A major revision to the current DoD Instruction 5000.2R, Operation of the Defense Acquisition, is awaiting signature for release.

1.1.5. Certifications and Compliance Testing

Section 8102 of the FY 2001, Defense Authorization Act requires that before Milestone I, II, III approval of major systems, the DoD CIO certify that the system is developed in accordance with the Clinger-Cohen Act. Draft DoD Directive 4630.5, Information Interoperability and Supportability, implements Clinger-Cohen and Public Law 105-261. It states that requirements for information interoperability will be characterized in a family of systems or system of systems joint mission area context for all IT and National Security Systems capabilities. It requires system dependencies and interface requirements be described in sufficient detail to enable test planning for information interoperability Key Performance Parameters (KPP).

1.1.6. Security

SECNAVINST 5239 (Draft), Department of the Navy Information Assurance (IA) Policy, outlines a defense in depth strategy for protection of DON information systems and requires that measures to ensure the confidentiality, integrity and availability of IT assets are based on mission criticality, required level of assurance, and classification or sensitivity of information processed, stored and transmitted. It also requires that DON IT and NSS system developers shall register and maintain their official metadata structures and definitions in the DON Data Management and Interoperability Repository for IA assessment and life cycle management. SECNAVINST 5239.3, Department of the Navy Information Systems Security (INFOSEC) Program, sets policy which states that data processed, stored and transmitted by information systems shall be adequately protected with respect to requirements for confidentiality, integrity, availability and privacy. Also, classified information processed or stored by DON information systems shall be safeguarded as required by that level of classification. Compliance with the policies outlined in these instructions is accomplished through the certification and accreditation process, application of IA throughout the life cycle of IT systems and training of individuals operating DON information systems.

1.2. DON Approach for Establishing DMI Infrastructure

In order to satisfy the governing directive discussed above, it is necessary to establish an infrastructure to focus disparate data management and interoperability efforts to:

- Aggregate requirements
- Focus resources on enterprise-wide problems
- Develop common approaches
- Build upon lesson learned

The DMI infrastructure has two components:

- Management Component: DON CIO, ASN (RDA), Navy and Marine Corps Data Administrators, Board of Representatives, and the DMI Management Board which includes the Functional Data Managers.
- Engineering Component: DON Data Architecture which includes information requirements and models; and the DON DMI Repository which includes a systems catalog, systems database structures, data element definitions, transfer formats and standards, and data sources and users.

The DMI infrastructure needs to address data as a corporate asset; this includes databases and data that is embedded in applications. At the May 1999 DON CIO Board of Representatives meeting, several attending CIOs, including those representing CINCLANTFLT and CINCPACFLT, stated that a global connectivity and common computing environment are essential, but not sufficient for Network-Centric Warfare. This resulted in the Office of the DON CIO developing both a draft Strategic Plan and SECNAVINST for DMI. These documents were used as a basis for an Integrated Product Team, composed of representatives from 28 commands, who validated the plan and the instruction and developed this Implementation Planning Guide. The guide is intended to provide a foundation for DON DMI implementation in a rapid and consistent manner as part of ongoing strategic initiatives, including NMCI, IT-21, and the ERP pilots.

Exhibit 8, DON DMI Mission, shows that data management is essential to information management and knowledge management. DMI will be executed through established requirements, PPBS and acquisition processes.

DON DMI MISSION

Provide the data management and interoperability infrastructure and the processes to enable systems interoperability, knowledge management and information assurance.

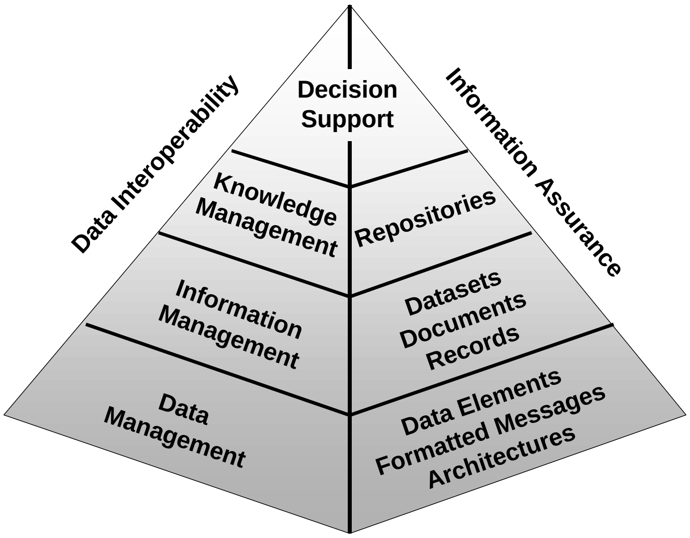


Exhibit 8. DON DMI Mission

The DMI approach is to refocus existing resources to:

- Identify and integrate user and system data requirements,
- Register existing systems data elements to use in developing baseline standards,
- Institute and manage data standards within the DON,
- Implement approved standards in all IT and NSS systems, and
- Provide consistent authoritative reference data.

The DMI will:

- Provide infrastructure and management oversight for implementation of the Clinger-Cohen Act and related mandates
- Provide a process for improved operational effectiveness, reduced data costs and return on investment
- Provide a process to achieve domain and enterprise-level interoperability to support JV2010 goals of information dominance

- Provide a process to support the capital planning process and IT assessment
- Establish training requirements for IT workforce
- Support data quality through the reduction of duplicate and inconsistent information

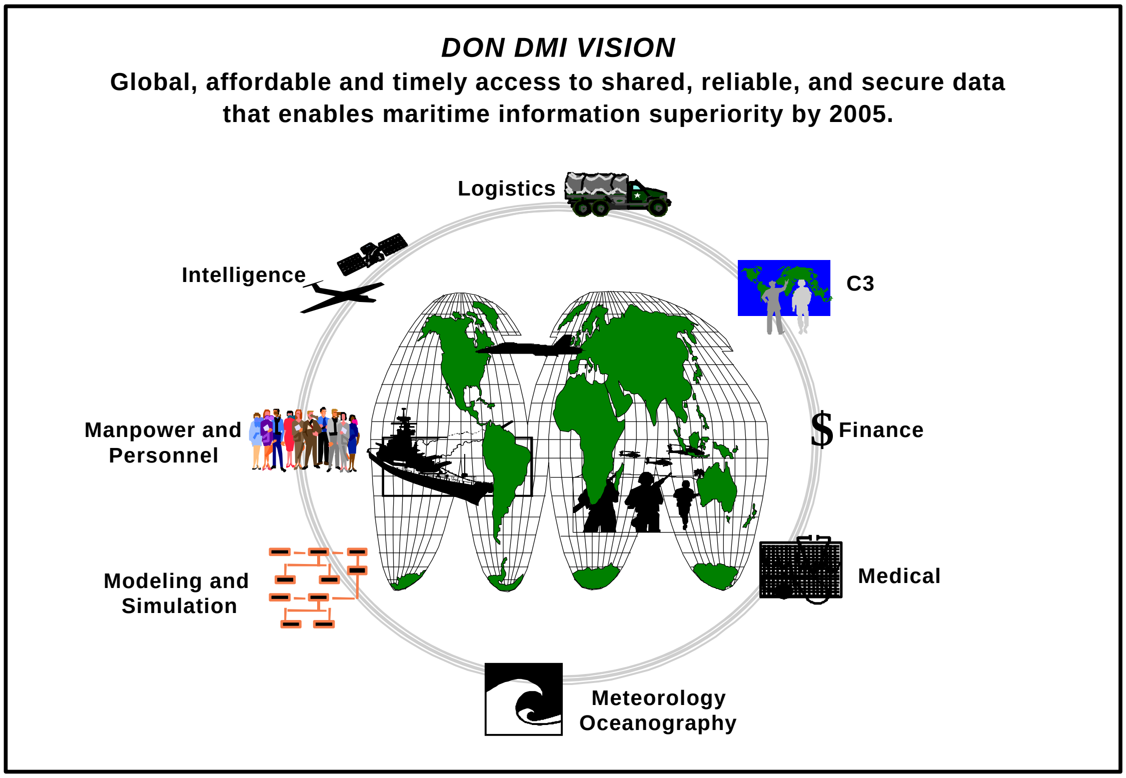
The DMI does not:

- Dictate hardware or software for systems use,
- Dictate system applications, or
- Dictate internal system data processing.

1.2.1. Strategic Plan Provides the Vision

The DON Strategic Plan sets forth five major goals with supporting objectives and measures of performance. The plan is necessary to achieve the DON's mission and business objectives. DMI is needed to pave the way for an integrated, interoperable IT infrastructure.

Exhibit 9, DON DMI Vision, sets an ambitious schedule for two reasons. First, it is not possible to predict when the next engagement will occur; and second, the time is now if DON is leverage the ongoing IT-21, NMCI, and ERP efforts. There are not sufficient funds to do everything twice.



DON DMI VISION

Global, affordable and timely access to shared, reliable, and secure data that enables maritime information superiority by 2005.

Exhibit 9. DON DMI Vision

1.2.1.1 Goals

The DON DMI goals are:

1. Provide a DMI infrastructure that will ensure maritime information superiority.
2. Reduce the life-cycle cost of data through integration, standards, and the use of Authoritative Data Sources.
3. Provide a DMI Repository and tools to support assessments and engineering.
4. Provide a Data Architecture that addresses both information requirements and data capabilities.
5. Provide processes and metrics to enable and evaluate data management and data engineering.

1.2.1.2 Guiding Principles

While the vision and goals of DMI are important steps in defining the CONOPS, a number of guiding principles are needed to maintain focus. The following statements are consistent with the vision and goals:

- Data is created to meet specific information requirements that support specific missions and functions.
- Data quality in terms of timeliness, accuracy and completeness is directly dependent on mission requirements.
- Facts, as data, are entered once by authoritative data producers and reused across the enterprise.
- Data is managed as an enterprise asset.
- Data Management is the foundation for Information Management, Knowledge Management and Decision Support.
- Data management efforts are coordinated across organizations and programs.
- Adequate resources are applied to data management and data architecture activities.
- Data structure and standards are a major consideration throughout systems acquisition and life cycle maintenance.
- Data element standards are used to achieve systems interoperability at the data levels.
- Data element standards will be system-based and pragmatic.
- Information assurance policies apply to data management and interoperability and include security requirements for confidentiality, integrity, availability and privacy of metadata, domain values and instance data fill.

Without these principles, it is difficult to maintain a clear, consistent perspective on what DMI is intended to accomplish. With these concepts in place, we can discuss the high-level concept of operations for the DMI infrastructure.

1.2.2. SECNAVINST for DMI Establishes Policy and Assigns Responsibility

SECNAVINST 5000.X, DON Data Management and Interoperability, is the DON policy on data management that implements DoD policy. The policy goes well beyond the data standardization approaches of the past. The SECNAVINST calls for a joint Navy and Marine Corps implementing instruction/order and supporting implementation plans that will ensure a robust DON DMI infrastructure.

Exhibit 10, DMI Interrelationships, shows the DMI organization as depicted in SECNAVINST 5000.X. Not shown but required is a Program Management Office to support the infrastructure and a DMI Management Board comprised of the DON CIO, Service Data Administrators and Functional Data Managers to provide guidance and resolve issues that go across organizational boundaries.

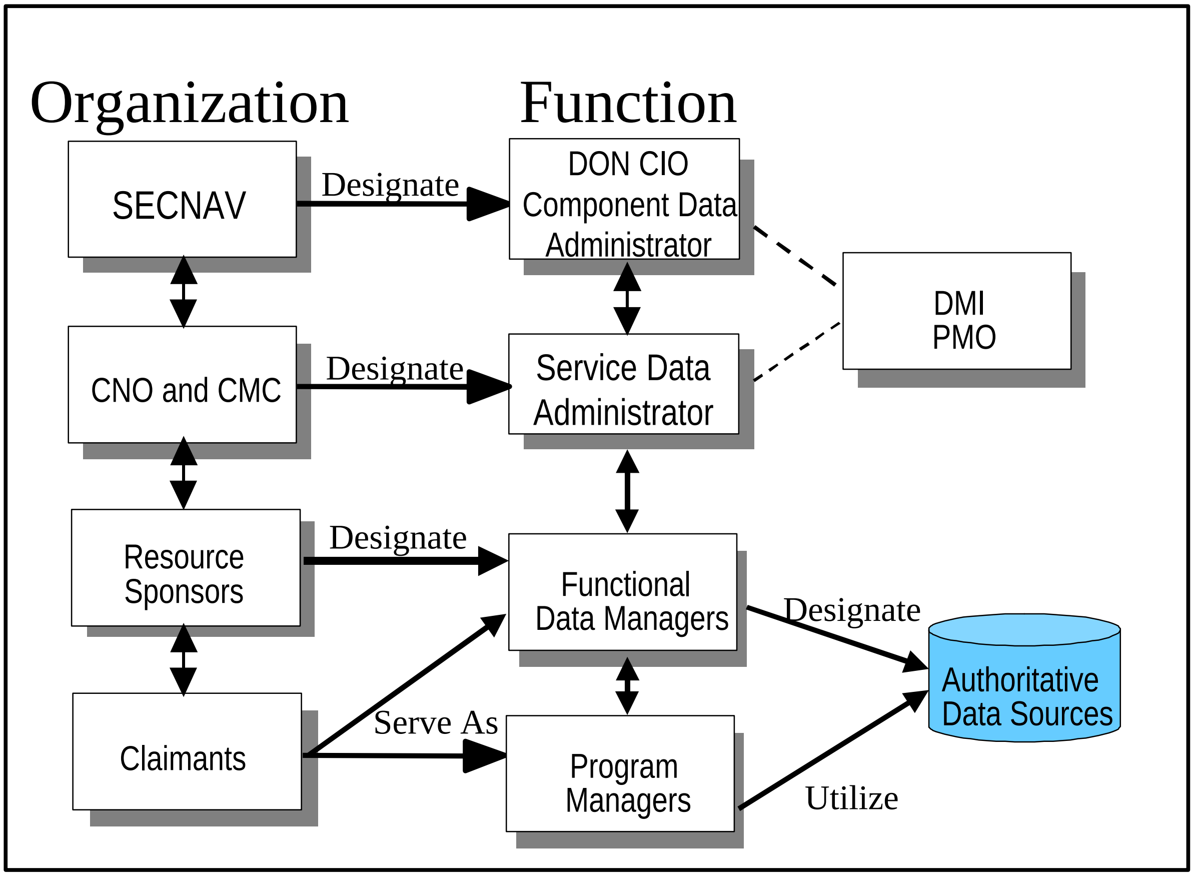


Exhibit 10. DMI Interrelationships

1.2.2.1 DON CIO/Component Data Administrator

The DON CIO is designated as the Component Data Administrator (CDAd) to implement DoD Directive 8320.1 responsibilities for data standards development and maintenance.

1.2.2.2 Navy and Marine Corps Service Data Administrators

The DON is a unique Department with the DoD as it contains two Services, The US Navy and the US Marine Corps and in time of war a third, the US Coast Guard. Therefore, the SECNAVINST for DMI establishes Navy and Marine Corps Service Data Administrators (SDAd) to:

- Support the DON CIO with the development and maintenance of the DON DMI Strategic Plan;
- Develop and maintain a Joint (two-Service) DMI implementation plan to resolve systems data interoperability and cross-functional issues; and
- Ensure Service organizations are kept current on data management issues and methodologies and provide appropriate training.

1.2.2.3 Resource Sponsors

Resource Sponsors are functional area managers, e.g., N1 for Personnel, N4 for Logistics, etc. The SECNAVINST for DMI requires Resource Sponsors to identify Functional Data Managers (FDM). It is believed in most cases that FDMs will equate to major claimants for the functional areas essential to warfare and warfare support systems acquisition, or for producing authoritative reference data that is used by those systems. Exhibit 11, DON DMI Functional Areas, provides a list of functional areas that was derived from Navy resource allocation. Eight areas are designated as primary based on the organization of the OSD Principal Staff Assistants (PSA), the DoD Data Administration functional organization, and lessons learned.

Resource Sponsor	Resource Area	Functional (SME)* Area Examples	Functional Data Managers (designated by Resource Sponsor)
Assistant Vice Chief of Operations (N09B)	Admin/Physical Security	Administration, Physical Security, Public Affairs, Legislative Support	
DCNO for Manpower and Personnel (N1)	Personnel Support	Manpower, Personnel	
Director, Naval Intelligence (N2)	Intelligence	Intelligence, Cryptology	
DCNO Fleet Readiness and	Logistics (including Sealift)	Sealift, Supply, Maintenance,	

Resource Sponsor	Resource Area	Functional (SME)* Area Examples	Functional Data Managers (designated by Resource Sponsor)
Logistics (N4)		Ordnance, Facilities, Environmental, Safety, Readiness	
Director, Space and Information Warfare (N6)	Space, Command and Control	Information Transfer, Command and Control, Space, Information Warfare, Modeling & Simulation	
DCNO Warfare Requirements and Programs (N7)	Warfare Programs, Naval Training and Education	Expeditionary, Surface, Submarine and Air Warfare; Training and Education	
DCNO Resources, Requirements, and Assessments (N8)	CINC Programs, Special Programs	Financial, Assessments	
Director, Navy T&E and Technology Requirements (N091)	RDT&E	Scientific and Technical, Test and Evaluation	
Director, Naval Medicine/Surgeon General (N093)	Medical Support	Medical	
Director, Naval Reserve (N095)	Reserve Affairs	Reserve Requirements	
Oceanographer of the Navy (N096)	Oceanography and Meteorology	Oceanography, Meteorology, MC&G	
Director of Religious Ministries/Chief of Chaplains (N097)	Religious Support	Religion	
Director, Naval Nuclear Propulsion Program (NOON)	Nuclear Propulsion	Nuclear	
Headquarters, Marine Corps	USMC Resources	Administration, Physical Security,	

Resource Sponsor	Resource Area	Functional (SME)* Area Examples	Functional Data Managers (designated by Resource Sponsor)
		Public Affairs, Legal Affairs, Legislative Support, Manpower, Personnel, Intelligence, Cryptology, Logistics, Information Transfer, Command and Control, Information Warfare, Modeling & Simulation, Training and Education, Test and Evaluation	

Exhibit 11. DON DMI Functional Areas

1.2.2.4 Functional Data Managers

FDMs are responsible for developing functional data architectures and data standards in coordination with system developers that are responsible to mission requirements. FDMs shall:

- Implement functional processes to produce and monitor the use of data within functional activities, information systems, and computing and communications infrastructures;
- Assist program managers and other systems developers in registering system database metadata and maintaining the metadata baseline;
- Develop and maintain functional area views of the DON data architecture;
- Develop candidate DoD standard data elements in coordination with the respective DoD Functional Data Administrator (FDAd) and the DON CDAd; and
- Designate Authoritative Data Sources (ADS) and maintain that designation in the DMI Repository (DMIR) using processes and procedures approved by the DON CIO, for their respective areas.

Previous Navy efforts to manage data as an enterprise asset have not achieved great success, primarily due to lack of dedicated resources and fewer tools for monitoring compliance with existing policy. Recognizing that budgets and those persons/agencies with control over the budget are key to success in almost any program, the DMI aligns the FDMs to Resource Sponsors. The Planning, Programming, and Budgeting System (PPBS) is a cyclic process that provides operational commanders the best mix of forces, equipment, and support attainable within fiscal constraints. The goal is to have an enforcement mechanism, tied to the PPBS process and acquisition milestone review process, to ensure necessary resources to comply with the requirements of the DMI are included in operating budgets and system acquisition programs. The intent of assigning resource sponsors as responsible for the assignment of the Functional Data Managers is to ensure that data management requirements are tied back to where an organization's dollars come from.

1.2.2.5 System Developers

System developers are responsible for implementing data standards where they exist, and supporting FDMs to develop them where they do not. System developers, assisted by FDMs, shall register systems metadata in the DON DMI Repository. This “knowledge capture” is intended to support systems design/migration systems engineering, and standard development and implementation necessary to systems interoperability at the data level.

1.2.2.6 Program Management Office

The DON CIO will identify a program management office for DMI. This office will support the DON CIO and Service Data Administrators in implementing and maintaining the DMI infrastructure. This will be a joint Navy and Marine Corp PMO, established to fill an Enterprise need to get the program started and maintained as was done with PEO IT, the Electronic Business Office, and Smart Card.

1.2.2.7 DMI Management Board

The DON CIO will establish a DMI Management Board. The Board will be comprised of the DON CIO, the Navy and Marine Corps Data Administrators, and the Functional Data Managers. It will be the authoritative body for addressing issues that cross functional areas and organizations.

1.2.3. SECNAVINST 5000.2B Revision Incorporates Common Data Documentation and Registration into Acquisition

DMI will be successful only if it is integrated into the acquisition process and provides program managers a value added over their current way of acquiring and maintaining data.

The SECNAVINST 5000.2B titled "Implementation of Mandatory Procedures for Major and Non-Major Information Technology Acquisition Programs" provides policy and guidance to commands and program managers for the procedures to follow for Major Defense Acquisition Programs (MDAPs) and Major Automated Information Systems (MAISs). Revision to this instruction would ensure that program managers and systems developers aggressively consider data standardization requirements of the DMI during the acquisition of all ACAT programs. Further, changes to the instruction would ensure that DMI related costs and necessary resources are being reviewed at each milestone decision briefing. Regular reviews will guarantee that program developers identify resources to use existing data standards and register their system's metadata into the DON DMI Repository.

Exhibit 12, Systems Data Registration Supports Business Process Reengineering, shows the application of the registered systems metadata and interface information that is critical to establishing and maintaining an IT baseline. Data costs can not be managed, nor can reliable, consistent interoperability be achieved if the foundation for all applications is not visible.

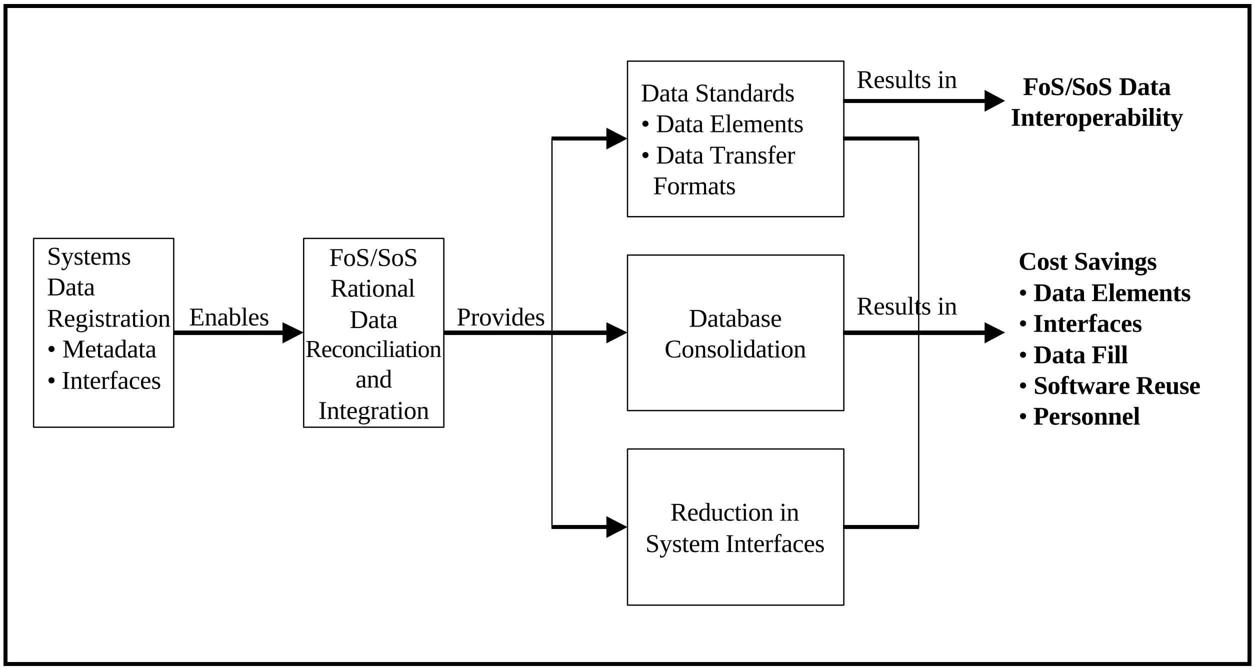


Exhibit 12. Systems Data Registration Supports Business Process Reengineering

1.2.4. DON DMI Repository Captures Systems Information Requirements and Business Rules

In order to manage data as a corporate asset, the DON, in accordance with guidelines established by the DON CIO, will build a DMI Repository, a web-enabled library of systems metadata recorded to show the metadata required to support Clinger-Cohen Act implementation. Its holding will include information about existing systems including systems database structures, data element formats and definitions, system data interface descriptions, and. data and process models. Imbedded within legacy system data structures are the business rules that support data mining and index design for internet navigation and demand pull. The repository also will hold "as is" and "to be" data architectures. Exhibit 13, DON DMI Repository Supports Enterprise Data Management, shows some of the intended repository applications.

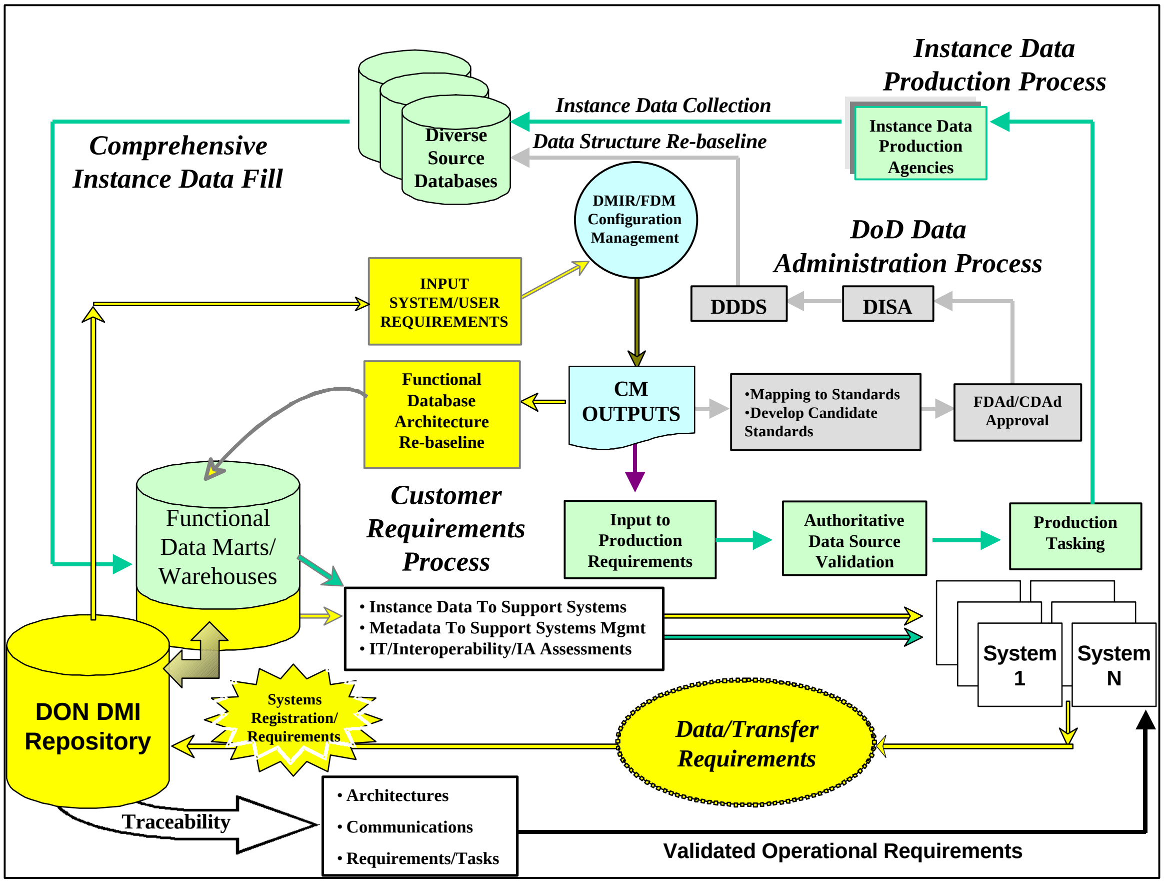

Instance Data Production Process
Instance Data Production Agencies
Instance Data Collection
Data Structure Re-baseline
Diverse Source Databases
Comprehensive Instance Data Fill
DMIR/FDM Configuration Management
DoD Data Administration Process
DDDS
DISA
INPUT SYSTEM/USER REQUIREMENTS
Functional Database Architecture Re-baseline
CM OUTPUTS
•Mapping to Standards
•Develop Candidate Standards
FDAd/CDAd Approval
Functional Data Marts/ Warehouses
Customer Requirements Process
Input to Production Requirements
Authoritative Data Source Validation
Production Tasking
• Instance Data To Support Systems
• Metadata To Support Systems Mgmt
• IT/Interoperability/IA Assessments
System 1
System N
DON DMI Repository
Systems Registration/ Requirements
Data/Transfer Requirements
Traceability
• Architectures
• Communications
• Requirements/Tasks
Validated Operational Requirements

Exhibit 13. DON DMI Repository Supports Enterprise Data Management

The DMI Repository is a key component of the DON approach for responding to the requirements of Clinger-Cohen. It is much more than a dictionary system. It shows data used by systems/applications in context. It is the primary tool that enables IT assessments and architecture and standards required by Clinger-Cohen Act and Section 8102 certifications.

The information in the repository will be available to system developers to reduce development costs of new systems and to enable better understanding of other systems with which they are required to interoperate. The repository will use a portal approach that will be centrally managed by the PMO but distributed among the FDMs for systems registration and maintenance of their respective functional areas. It will be accessed via the web using NIPRNET and SIPRNET. Information security requirements drive this dual access approach.

Capturing the structures of data and their entities and attributes (metadata) as implemented in operational systems provides a baseline to:

- determine data inconsistencies,
- assess data redundancies,
- improve interoperability,

- ensure data requirements are included in a system being developed to replace a legacy system, and
- support collaborative data standards development. Developmental data packages will be submitted to DISA for inclusion in the Defense Data Dictionary System (DDDS) after Navy and Marine Corps consolidation and prioritization of requirements.

1.2.5. DON Data Architecture Provides a Deterministic Framework of Models for Defining and Managing Standard, Interoperable Data Across DON

The DON CIO is responsible for developing and publishing the enterprise view of data and its management. This is responsive to Congressional and OSD mandates to achieve interoperability through measures that emphasize data standards. The DMI infrastructure and its operating concepts represent a unified program that pulls together and reconciles diverse efforts of data development and definition. Key to the success of this infrastructure and reconciliation is the DON Data Architecture.

The DON Data Architecture is a framework for organizing and managing the inter-relationships of data. This framework contains the optimal design of the data based on top-down and bottom-up analysis of all data requirements and capabilities in the DON enterprise structured and modeled according to DOD data standards guidance. It also contains the specific details regarding the actual implemented structure of data.

Exhibit 14, DMI Data Models, describes the various models comprising the DON Data Architecture. These models are based on the ANSI SPARC schema definitions. Each model in the architecture framework provides value and support to the DMI infrastructure and to DON's goals to achieve interoperability and information superiority. Section 2.5 describes how these models are developed and integrated.

Model Name	Characteristics	Value
• DON Enterprise Conceptual Data Model	• Top-down context of DON's information requirements • High level super entities non-attributed • Aligned with DoD Data Architecture	• Enterprise consensus on DON Data Requirements • Organizing Framework for logical modeling and standards
• DON Enterprise Integrated Logical Data Model	• Bottom-up data requirements/capabilities driven • Reconciled across the Enterprise • Standardized • Attributed	• Provides semantic consistency across DON Enterprise • Enables system development across the Enterprise (cross-functional)

Model Name	Characteristics	Value
	• Reconciled with DON Enterprise Conceptual Model • Integration of Functional Area Logical Data Models	• Identifies dependencies and interrelationships that are cross-functional • Enables development of DON FoS and SoS views traceable to DoD framework
• Functional Area Logical Data Model	• Bottom-up functional area data requirements/ capabilities driven • Represents the sum of data requirements/ capabilities • Establishes the criteria that an ADS must meet to satisfy the production requirements of the functional area • Reconciled across the functional area • Standardized • Attributed	• Functional area consensus on DON data requirements • Context for system design and standards compliance • Enables development of Families of Systems within the functional area • Identifies the sum of instance data production required across the functional area
• System Logical Data Model	• Based on system's data requirement • Standardized (developmental, candidate, approved) • Logical structure of physical data • Attributed • Defines implementation of business rules used by the system	• Enables development of FoS within the functional area • Enables system to system comparison for analysis of capabilities for redundancies redundant and gaps • Supports acquisition decisions to show current • Contributes to the development of the functional area LDM • Provides system justification for instance data production • Supports system development by promoting reuse of current systems capabilities

Model Name	Characteristics	Value
• System Physical Data Model	• Represents the physical implementation of data within the hardware and physical storage • Structure of table names, data element access names, domain values, etc…	• Promotes code reuse across the DON • Supports information exchange design

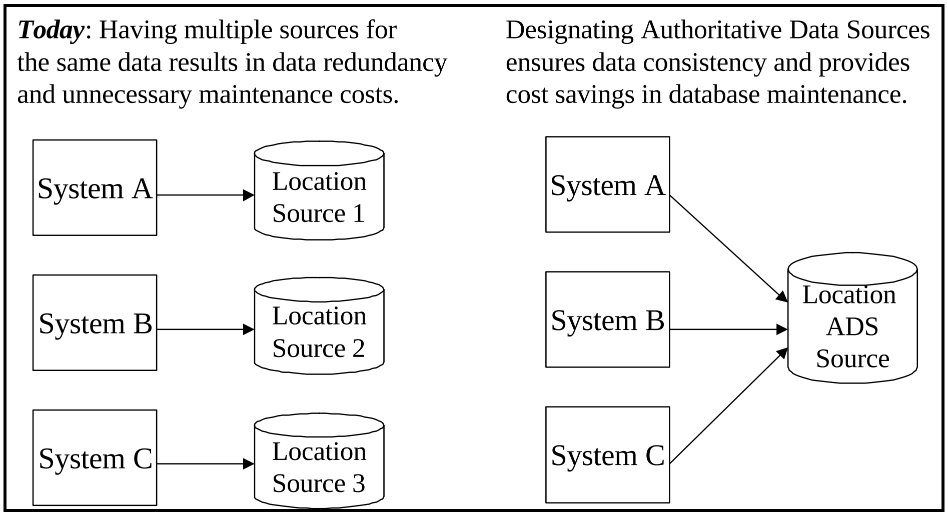
Exhibit 14. DMI Data Models

1.2.6. Authoritative Data Sources Enable Improved Decision Support and Cost Savings

The purpose of designating Authoritative Data Sources (ADS) is to ensure system developers and their support activities have consistent instance data for population of new and current systems and applications. The FDM will assist developers and support activities in determining which source provides the most complete, most current, and most accurate data to support developmental and implemented systems' requirements.

ADSs are the data products, including databases that have been identified, described and designated by appropriate FDMs for DON data support. When we use the term ADS, we are referring specifically to the actual database that provides the instance data, which we distinguish from the ADS Producer, the agency or organization charged with the responsibility for maintaining the ADS Database. The purpose of specifying an ADS is threefold.

First, to identify the most authoritative sources of specific data in terms of completeness, accuracy, and currency; and thereby eliminating multiple, possible inconsistent and inaccurate sources of data as depicted in Exhibit 15, Authoritative Data Source.



Today: Having multiple sources for the same data results in data redundancy and unnecessary maintenance costs.

Designating Authoritative Data Sources ensures data consistency and provides cost savings in database maintenance.

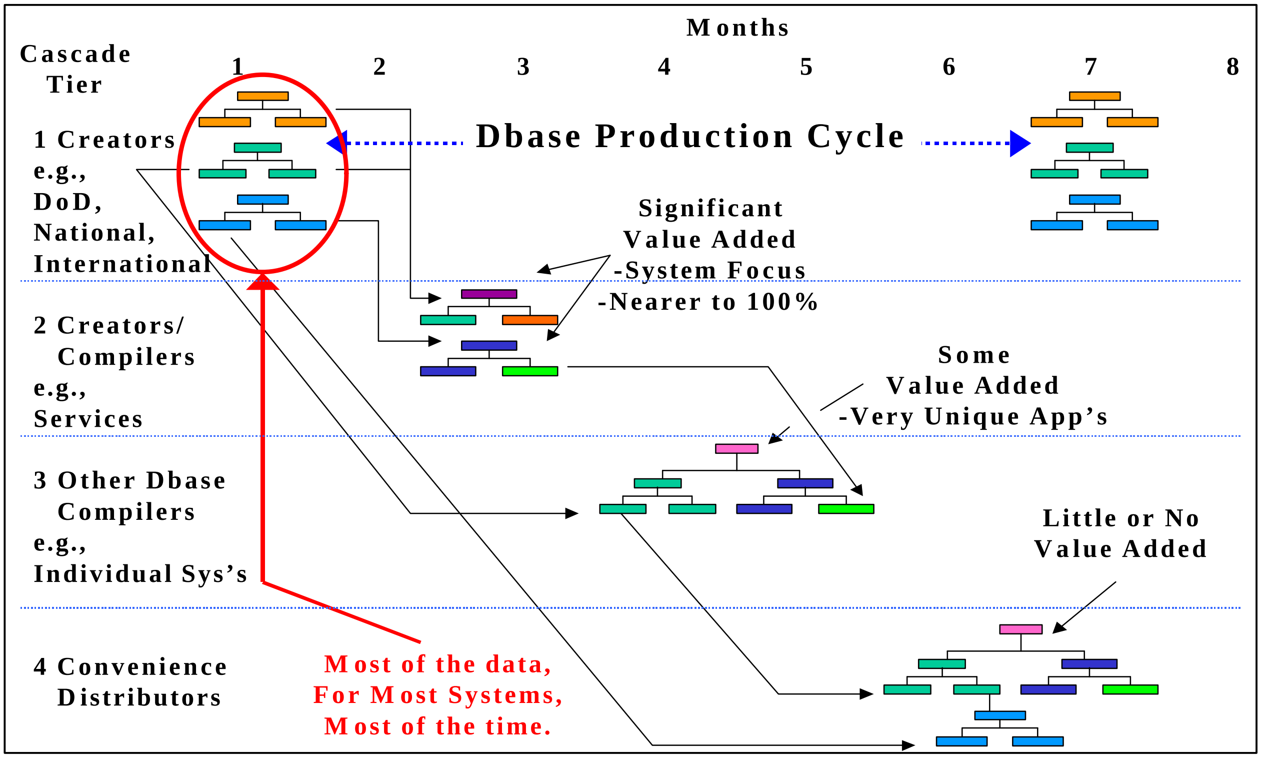
Exhibit 15. Authoritative Data Source

Second, to ensure version control and integrity of the database contents and manage the periodicity (i.e., synchronization) of updates to users.

Third, to control the negative effects of reference data cascading while taking advantage of its value-added contributions.

Reference data cascading results when data produced at one tier is repackaged and redistributed at lower data production tiers as illustrated in Exhibit 16, Reference Data Cascading.

There are some cases in which the Data Cascading effect results in a value-added product. For example, data produced at Tier 1, the national or DoD level of production, often solves "most of the reference data requirements, for most systems, most of the time." The value added by supplementary instance data production, data tailoring and data focusing, at Tier 2, most often at the Service level, results in an improved database product. Below Tier 2 we find that the value added is marginal, and below Tier 3 there is usually no value added. We refer to these lower-tier initiatives as "Convenience Distributions" as their purpose is often to only aggregate multiple sources of data under a common access front-end. Also, data production below Tier 3 presents the inherent danger of unintentional data aging and/or obsolescence because higher tier data has been refreshed through its normal update cycle, but lower tier data continues to reflect the older data instances. The effect is that these lower tier efforts might unintentionally be disseminating obsolete or completely erroneous information to their consumers.



Months
Cascade Tier
1
2
3
4
5
6
7
8
Dbase Production Cycle
1 Creators e.g., DoD, National, International
Significant Value Added -System Focus -Nearer to 100%
2 Creators/ Compilers e.g., Services
Some Value Added -Very Unique App's
3 Other Dbase Compilers e.g., Individual Sys's
Little or No Value Added
4 Convenience Distributors
Most of the data, For Most Systems, Most of the time.

Exhibit 16. Reference Data Cascading

In both cases, that of multiple sources and that of reference data cascading, the effect on the end user is a general inability to differentiate between these data sources to determine the best source for their unique systems application. Absent practical guidelines for authoritative source selection different users have historically selected different sources containing different data instances. When these data are exchanged within a network-centric environment, the result is an inability on the part of automated systems to resolve the inevitable and numerous data conflicts that occur. As a result, decision support, situational awareness, combat identification, and other critical measures of systems performance are seriously degraded or rendered completely ineffective.

The identification and use of ADS will result in a significant return-on-investment by:

- Eliminating unnecessarily duplicative sources of instance data production.
- Eliminating unnecessarily duplicative distribution of ‘repackaged’ data.
- Promoting consistent cross-system exchange and correlation of common data instantiations, thereby improving system performance.
- Promoting data synchronization (same instance of data being used by similar systems at the same time), thereby improving system performance.
- Providing a well-defined process for system developers, program managers, and other end users to identify authoritative data sources for specific systems and applications.
- Making it feasible to merge and combine data from different sources to answer strategic queries, to perform data mining, and to support decision-support.

1.2.7. Conformance Testing Ensures Interoperability and Rational Data Standards

Title 10 designates the DoD CIO responsibility for ensuring the interoperability of IT and NSS throughout the DoD, and assigns Military Department CIOs responsibility for ensuring that IT and NSS are interoperable with other relevant systems of the government and the DoD. The objectives are 1) to achieve, through an outcome-based process, an interoperable, integrated, and secure universal IT and NSS infrastructure, and 2) to achieve not only joint (inter-Service) interoperability, but also combined and coalition interoperability.

Draft reissue DODD 4630.5, Information Interoperability and Supportability states it is DoD policy that:

- The Department will achieve and maintain Information Superiority in support of the warfighter and decision-maker. To achieve Information Superiority, the DoD must develop, acquire, maintain and exploit interoperable IT and NSS. Joint and combined forces must be supported through interoperable IT in global operations across the peace-conflict spectrum. For the purposes of this Guide, all IT and NSS developed for use by US forces are for joint, combined and coalition use.

Draft reissue DODI 4630.8, Information Interoperability and Supportability, states the Director of Operational Test and Evaluation, shall:

- Develop policy and process to ensure IT and NSS are tested early in the acquisition cycle, and with sufficient frequency during a capability's life to verify information interoperability key performance parameters (KPPs), and to assess overall information interoperability.
- Ensure all IT and NSS program documentation and performance results are reviewed to determine criticality of information interoperability requirements to mission accomplishment and assess if information interoperability requirements are being met.
- In conjunction with USD (AT&L), the DoD CIO and the Joint Staff, identify information interoperability deficiencies existing in program documentation and performance results.
- Establish an Interoperability Watch List for those IT and NSS for which information interoperability is deemed critical, but insufficient evidence exists that interoperability issues are being addressed.
- Coordinate with Joint Forces Command to develop and apply outcome-based metrics for operational test and evaluation of information interoperability KPPs.
- In coordination with Joint Forces Command, sponsor Joint Test and Evaluations (JT&Es) for the identification and verification of information interoperability shortfalls and issues.

Testing is a management tool to ensure not only compliance with standards but also as a means to determine what standards are rational. Creation of data standards without an adequate systems baseline and testing to determine the utility of new standards and how they interact with existing standards can result in both ineffective and inefficient standards. This applies for both data elements and data transfer formats.

1.2.8. DMI Education and Training Supports Consistent Implementation and Sustainment

Data Management is not well understood. It is often perceived as something very down in the weeds or something that can be done by a computer alone. One of the major lessons learned in the DoD Data Administration process to date is that DoD is large and complex and the data standards approach must be system based and pragmatic.

In order to maximize DMI within the DON and satisfy goals within DoD and DON Strategic Plans, the Service Data Administrators, supported by the PMO, must establish and implement a training plan that addresses the development and sustainment of core DMI capabilities. The plan is intended to satisfy the strategic goal as established in Goal 8 of the DON IM&IT Strategic Plan. DMI education and training must include "school house," interactive and remote, and on-the-job components. The plan must accommodate training provisions at all levels to obtain a common vision in order to achieve and maintain information superiority.

1.2.9. DMI Outreach Provides for Joint, Combined, and Coalition Interoperability Planning and Technology Insertion

The DON CIO and Service Data Administrators will institute a DMI Outreach strategy to ensure effective information flow and partnerships with DMI organizations and efforts in other services, agencies, industry and foreign countries. After the Gulf War, an Army lead Advanced Concept Technology Demonstration (ACTD), C4I for Coalition Warfare, justified message development because of an inability to pass command and control information between nations except by liaison officer, facsimile, telephone, or loaning equipment.

Outreach is a way to maximize jointness. It is less expensive and more effective for FDMs to work with their joint counterparts and other service partners to design joint and combined data integration efforts as a means of assuring joint and combined interoperability as well as interoperability with the Coast Guard in time of war. In a like manner, there is much to be learned from our foreign partners. They have been working with less resources and as a result are developing standards based processes that do not require common hardware or software. It also is important to work with industry to be aware of new technologies and to make industry aware of DON information requirements. IT has the potential for exponential increase in effectiveness provided it is harnessed and uniform in its implementation.

1.2.10. DMI Evaluation Process Provides the Measures of Performance and Metrics to Assess ROI

There are three basic reasons for measuring DMI performance: understanding, predicting and controlling. From the understanding of what constitutes usual and unusual cases, a baseline can be established. Working from a baseline, predictions can be made regarding the accomplishment of specific tasks and operations that in turn aid in the understanding of which activities are most effective for achieving desired goals.

Establishing Measures of Performance (MOPs) or Key Performance Parameters (KPP) and a viable set of metrics assures visibility into the current status of DMI and enables process improvements to it. Metrics both support and validate the strategies and products specified for each of the DMI goals; they are essential to obtain an accurate view of the state of a project and to the effective and efficient management of it.

Ultimately, the purpose of establishing MOPs/KPPs and associated metrics is to improve the return-on-investment (ROI) on Information Technology (IT) investments and to achieve Information Superiority.

1.2.11. Joint Navy and Marine Corps Implementation Plan Provides the Work Breakdown Structure for Achieving the Vision

The SECNAVINST for DMI requires a Joint Navy and Marine Corps Implementation Plan. Section 2 of this Guide provides the DMI processes developed by the IPT. Section 3 provides a Plan of Action and Milestones (POA&M) that should be used as the foundation for developing a Work Breakdown Structure (WBS) for joint Navy and Marine Corps implementation.

1.3. Relationship to Other Architecture, Standards, and Infrastructure Efforts

Due to the pervasive nature of data, DMI is closely related to a number of other major information technology efforts. In many cases, these related efforts and DMI are complementary; for others, DMI is a prerequisite. This section provides an overview of the primary related efforts at the DoD and DON-levels, as well as closely-related commercial, national, and international activities.

1.3.1. Related DoD Efforts

Several major efforts initiated and led by DoD associated with information technology architecture, infrastructure, common operating environments, and data administration are directly related to DMI. This section summarizes the following efforts and their relationship to DMI:

- DoD Data Administration and Shared Data Engineering
- DoD Architecture Framework
- Information Interoperability and Supportability
- Global Information Grid

1.3.1.1 DoD Data Administration and Shared Data Engineering

The DoD Data Administration program was established in 1991 with the issuance of DoD Directive 8320.1. ASD (C3I) has designated the Defense Information Systems Agency (DISA) as the Executive Agent (EA) for the program. To facilitate the development of DoD data standards, DISA developed and maintains the Defense Data Dictionary System (DDDS). DISA also coordinates proposals for DoD Standard Data Elements as outlined in DoD 8320.1-M-1, “Data Standardization Procedures”. DISA represents ASD (C3I) by providing leadership as the DoD Data Administrator. Supporting the data administration program and the standardization process are Functional Data Administrators (FDAds), representing OSD Principal Staff Assistants, and Component Data Administrators (CDAds), representing the CINCS/Services/Agencies. The DON CIO, as DON CDAd, is responsible for:

- Managing DON Data Administration in accordance with the Directive and Procedures.
- Reviewing proposed changes to DoD Standard Data Elements and forwarding changes to the DoDDAd and appropriate FDAd.
- Identifying the interface between the users, database administrators, and application developers of the information systems within the DON and serve as the liaison to the DoDDAd and the FDAds.
- Representing DON interests to the OSD Principal Staff Assistants, the DODDAd, and the FDAds.
- Annually reviewing, updating, and submitting the DON portion of the DoD Data Administration Plan.

The product of the DoD program is the DoD Data Architecture, which consists of a collection of logical data model views for DoD functional areas and the associated metadata. The associated metadata is captured in the Defense Data Dictionary System (DDDS). DMI implements DoD Data Administration within the DON.

In addition to DoD Data Administration, a program that addresses data within the Defense Information Infrastructure (DII) Common Operating Environment (COE), known as SHAred Data Engineering (SHADE), provides a comprehensive strategy for mitigating data access, delivery, and interoperability problems. The COE Data Emporium was established to make available Reference Data Sets, Database Segments, and XML tags/metadata necessary to support the COE:

- Reference Data Sets provide standardized values for codes used across the DoD. Examples include Country Codes, Military Ranks, and Geolocation Types.
- COE database segments contain the data definition language (DDL) needed to create all or a part of a single database instance, including data stores and data objects.
- XML tags/metadata are being standardized for a number of Namespaces that support specific mission areas. These standard tag sets are available for re-use by developers implementing XML data exchange solutions.

Both Data Administration and SHADE are important components of an enterprise data management solution. Much of the DMI strategy is complementary to the existing data administration program.

1.3.1.2 DoD Architecture Framework

The Clinger-Cohen Act of 1996 (CCA) assigns CIOs the responsibility of "developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture (ITA)". Within DoD, Services and Agencies are required to follow the DoD Architecture Framework in the development of their respective ITAs. Framework version 2.1, currently in draft, identifies the architecture products that are developed within three separate, but interrelated views:

- Operational: a description of the tasks and activities, operational nodes, and information exchange requirements between nodes. A technology-independent view.
- Systems: a graphical and textual description of systems and interconnections used to satisfy the operational needs described in the Operational view.
- Technical: the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements.

Within the Operational view, logical data models are used to develop the high-level data requirements for support of the information exchanges identified in that view. Within the Systems view, physical data models are used to capture the representation of data within the systems that support operational requirements. The Technical view includes the specification of the standards that are used to ensure interoperability; data dictionaries and metadata specifications are an essential element of this view.

The capture of Framework products is supported by both the DON Integrated Architecture Database (DIAD) and the Joint C4ISR Architecture Planning System (JCAPS). The DIAD is complementary with the DON Data Management & Interoperability Repository (DMIR), which is currently under development.

1.3.1.3 Information Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)

ASD (C3I) is currently leading an effort to revise DoD Directive 4630.5 and DoD Instruction 4630.8. The previous emphasis of these policies was on interoperability between C4I and interfacing systems. The definition of interoperability was largely restricted to the ability of systems to exchange services with one another; in other words, physical connectivity. The revised policies define interoperability as the technical exchange of information, and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment.

In addition to codifying the role of Chief Information Officers in ensuring the interoperability of IT and NSS, the revised policies direct that interoperability will be assessed from the perspective of mission areas and families of systems. DMI supports the assessment of interoperability from this perspective. Functional Data Managers will define the families of systems that support their respective areas. Common data architectures for these families of systems will help achieve the level of information interoperability required by these policies.

1.3.1.4 Global Information Grid

In December 1998, ASD (C3I) established several working groups focused on defining the Global Networked Information Enterprise (GNIE), which later became know as the GIG. The GIG is described as the globally interconnected, end-to-end set of information capabilities associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. It includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996.

The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG is in the process of being described through a series of DoD Architecture Framework products, as defined by the GIG Architecture Integration Panel (GAIP). These products include:

- High Level Operational Concept graphic
- Operational Node Connectivity diagrams
- Operational Information Exchange matrices

- Command Relationship charts
- Activity Model

One of the goals of the GIG Architecture is to describe joint/enterprise missions and depict them in sufficient detail to allow DoD to address specific problems. The DMI FoS/SoS data architecture approach will support development of the GIG Architecture.

1.3.2. Related DON Efforts

- DON Information Technology Infrastructure Architecture
- Information Technology Standards Guidance
- Knowledge Management
- Information Assurance
- Navy Marine Corps Intranet (NMCI)
- Information Technology for the 21st Century (IT-21)
- Enterprise Resource Planning
- Electronic Business

The DON DMI program is key to other DON architecture and infrastructure efforts. It is an enabler of data interoperability between the various efforts.

DMI is key to a number of interrelated efforts that affect DON systems operations. Exhibit 17, DON DMI Within the ITA Environment, shows key information initiatives being brought to focus on DON IT systems and operations.

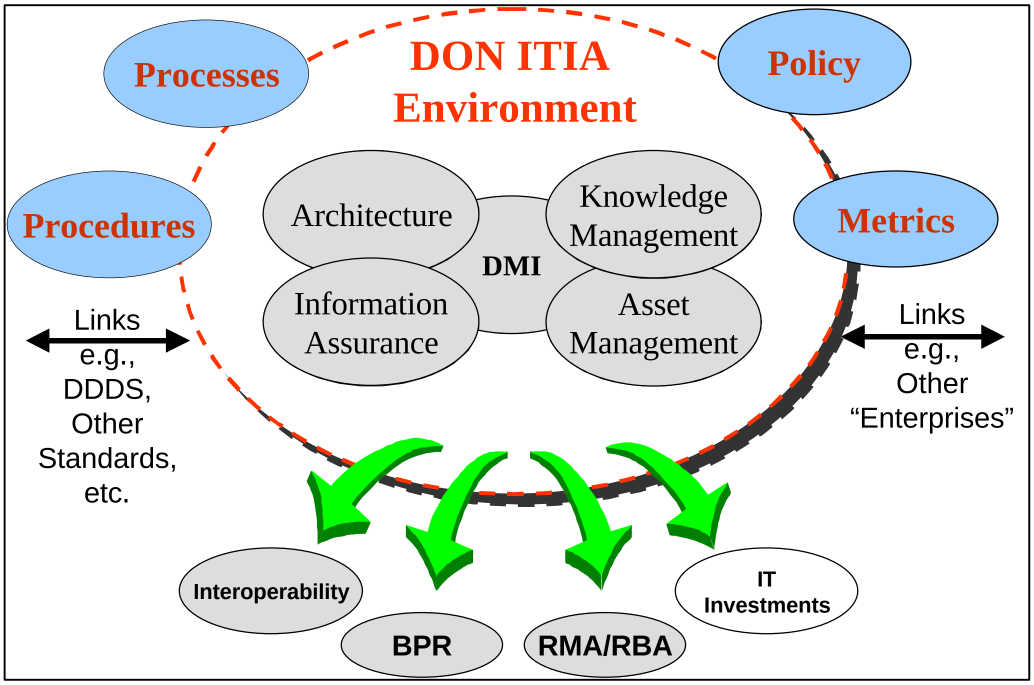


Exhibit 17. DON DMI Within the ITA Environment

1.3.2.1 Information Technology Infrastructure Architecture (ITIA)

The ITIA, like the DMI IPG, was developed under a charter of the DON CIO Board of Representatives. The objective was to establish standard templates for wide area networks (WANs) metropolitan area networks (MANs), campus area networks (CANs), and local area networks (LANs) as well as the supporting standards and protocols for network services. The ITIA is the "Technology Infrastructure" component of the DON Enterprise Architecture, as defined by the Office of Management and Budget in OMB 97-16. The ITIA serves as a foundation document for the architecture of the Navy Marine Corps Intranet (NMCI).

A robust infrastructure is essential to respond to today's information transfer demands. Without organizing our data assets through the use of comprehensive data architectures, the maximum benefits of this infrastructure will not be realized. DMI provides the means of achieving higher levels of information interoperability that cannot be achieved through connectivity alone.

1.3.2.2 Information Technology Standards Guidance (ITSG)

The DON Information Technology Standards Guidance (ITSG), Version 99-1 of 5 April 1999 identifies and describes IT specifications, standards, products and best practices for the DON based on an established criteria of security, functionality, interoperability, performance and cost. They are to be used in conjunction with the ITIA to ensure consistent planning, development and implementation.

The DON DMI program establishes the infrastructure and processes necessary to implement the data management and interoperability portions of Chapter 8 of the ITSG.

1.3.2.3 Knowledge Management (KM)

Information technology (IT), information management (IM), and DMI are essential to achieving information superiority. Knowledge Management (KM) offers the potential to significantly leverage the value of IT investments by providing the linkage between technology and people; it is a process for optimizing the effective application of intellectual capital to achieve organizational objectives. Underlying this definition are five basic tenets: technology, content, process, culture, and learning.

DMI supports KM in two areas: technology and content.

- Technology – technology facilitates and enables information transfer; DMI, through its contributions to information interoperability, ensures that information delivered is in a format that can be used by the receiver
- Content – a comprehensive data architecture facilitates consistent information content through the definition of standards for data that is shared across functional and operational boundaries.

1.3.2.4 Information Assurance

Information Assurance consists of information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation:

- Availability - Assuring information and communications services will be ready for use when expected.
- Integrity - Assuring information will not be accidentally or maliciously altered or destroyed.
- Authentication - Positively verifying the identity of sender and recipient of data.
- Confidentiality - Assuring information will be kept secure, with access limited to appropriate persons
- Non-Repudiation - Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processes the data.

Information protection measures that ensure these requirements are met are:

- Encryption – Converting understandable information into unintelligible data for storage and transport
- Access Control – Controlling access to system data and resources based upon user identity and operational role
- User Identification and Authentication – Securely determining user identity or operational role

- Malicious Content Detection – Examining incoming data to detect and block malicious content (e.g., viruses)
- Audit – Recording security-relevant events in a protected form
- Physical and Environmental Controls – Policies, procedures, and mechanisms related to physically protecting and providing for continuity of operations for system components.

DMI supports information protection measures in a number of ways: the use of data standards provides a means for conducting content detection; the documentation of database structures can be used to support analysis if databases in the event that an intrusion has occurred. This concept is discussed in further detail later in this document.

1.3.2.5 Navy Marine Corps Intranet (NMCI)

The Navy Marine Corps Intranet is an initiative for providing consistent, robust, secure, and reliable network services for the Navy and Marine Corps shore establishment. The PEO (IT) manages the NMCI program as well as DON Enterprise Applications. It is anticipated that the common IT infrastructure that NMCI will bring to the DON will provide the environment needed to facilitate major systems reengineering efforts. Current legacy systems will be evaluated and migration plans developed to reduce the numbers of redundant databases and outdated platforms.

The NMCI will ensure the interoperability of network connectivity and services. While this is a necessary step toward overall interoperability improvements, it is not sufficient on its own. The DMI program will enable the DON to achieve the maximum benefits of the network by addressing interoperability at the data level. Exhibit 3 shows the Levels of Information Systems Interoperability.

1.3.2.6 Information Technology for the 21st Century (IT21)

Network warfare, robust infrastructure and information dissemination to dispersed forces are all key elements to achieving information superiority. It was with this in mind that Information Technology for the 21st Century, or IT-21, was born.

IT-21 is a reprioritization of existing C4I programs of record focused on accelerating the transition to a PC-based tactical and support warfighting network. The goal of IT-21 is to link all U.S. forces and eventually even our allies together in a network that enables voice, video and data transmissions from a single desktop PC, allowing warfighters to exchange information that is classified or unclassified, and tactical or non-tactical. To do this, we must build a system to industry standards, using commercial off-the-shelf technology (or COTS), devoid of stovepipes, in a client-server environment that allows the pull of just what information is needed in a way that's seamless to the user in the field.

While the infrastructure provides connectivity, the levels of interoperability above domain and enterprise, shown in Exhibit 3, can only be achieved through the use of the management and engineering approaches that are part of the DMI concept of operations.

1.3.2.7 Enterprise Resource Planning (ERP)

In response to the “Reinventing Government” initiative, government agencies and the military services have accepted the challenge to become more efficient and effective in their business processes. Downsizing and shrinking budgets within the Department of Defense have made this a high priority within the Department of the Navy. The Department must maintain a balance between its operational forces and its supporting infrastructure as it works to transform its business practices. This infrastructure must remain flexible, responsive, and adaptable to the forces it supports. In December 1997, Secretary of the Navy John H. Dalton asked Under Secretary of the Navy Jerry M. Hultin to begin work on a DON strategic business plan as a means of addressing the need for reform in the business affairs of the Department. The result was the establishment of a Revolution in Business Affairs Executive Committee (RBA EXCOM). The RBA EXCOM chartered a Commercial Business Practices (CBP) Working Group. The CBP Working Group decided that the DON should use Enterprise Resource Planning as a foundation and/or lever for change.

ERP enables organizations to consolidate data in central corporate databases and adopt standard applications and business processes. ERP applications are commercial-of-the shelf (COTS) packages. As such, their database designs are optimized to support the applications; this poses two data administration challenges:

1. The entities and attributes are modeled according to the vendor’s standards.
2. Modifications to the database structures are not recommended.

The use of vendor naming conventions, data types, character length, domain values, and other metadata characteristics normally preclude the use of DoD Standard Data Elements. Mapping and matching of ERP data to DoD standards to support data interchange needs to be conducted to incorporate ERP data models into the Enterprise Data Architecture. Modifications to the ERP data structures, such as the addition of data elements or modification of data types, can be made but are not recommended. Any such changes are overwritten when new versions of the software are installed; the modifications must be re-applied at each upgrade.

ERP databases will become an important component of the Enterprise Data Architecture as Commands adopt the technology. The data administration issues are complex and must be coordinated across the DON to ensure interoperability with other DON, DoD, and Federal databases. These issues will be addressed through coordination between the EDIT, Functional Data Managers, and Service/Component Data Administrators.

1.3.2.8 Electronic Business

In 1990, the DON started to apply Electronic Business (EB) technologies in high-payoff areas, recognizing that many paper-intensive activities were not cost effective in light of technology that was becoming available. The current EB initiative seeks to build electronic information paths within the Department of the Navy, the larger Defense community, other government agencies, and our commercial partners. However, EB is more than only automating manual processes and eliminating paper transactions – EB will move the DON into an enterprise-wide electronic business environment and fundamentally change the way we operate by applying Business Process Reengineering (BPR).

EB is a philosophy for conducting business in an integrated and automated paperless information environment. Its software and hardware tools include Extensible Markup Language (XML), Electronic Data Interchange (EDI), E-mail, Electronic Funds Transfer (EFT), Navy-Marine Corps Intranet (NMCI), SmartCard, and other web technologies. Both the DoD and the DON seek to apply these technologies in high-payoff areas to improve processes and reduce expenses. When used properly, EB is a source of significant strategic advantage, and will transform business relationships as we know them within the Defense community and among DoD, other government agencies, and commercial entities. After improving our business processes through reengineering and adoption of best business practices, applying these technologies with an objective of web-engineering every application, is crucial to achieving the efficiencies possible.

DMI will support the reengineering efforts associated with EB by providing the processes for documenting the AS-IS data architecture. The establishment of data standards to support XML and EDI transactions is essential to the success of EB initiatives.

1.3.3. Related Commercial, National, and International Efforts

Data standards efforts at the National and international levels, as well as in the commercial sector, have a significant impact upon the data management practices of the DoD enterprise. Global connectivity provides wider opportunity to exchange data with Allied and coalition partners, commercial partners, and other Agencies of the Federal Government. Some of the major efforts that require DON representation/monitoring include, but are not limited to:

Commercial:

- Organization for the Advancement of Structured Information Standards (OASIS)
- Meta Data Coalition
- Object Management Group

Federal:

- Chief Information Officer’s Council XML Working Group

International:

- International Organization for Standardization (ISO) Technical Committees

2. DMI CONCEPT OF OPERATIONS

The DMI infrastructure consists of both management and engineering components. To implement and sustain DMI across the DON requires senior management commitment; modifications to existing acquisition requirements; and a robust infrastructure with adequate funding, data management tools, and consistent procedures. Section 1 addressed the "what" and "why" of DMI; this section addresses the "how" for DMI implementation and sustainment.

Exhibit 18, DON DMI Concept of Operations, shows that DON DMI has five distinct, yet interrelated components:

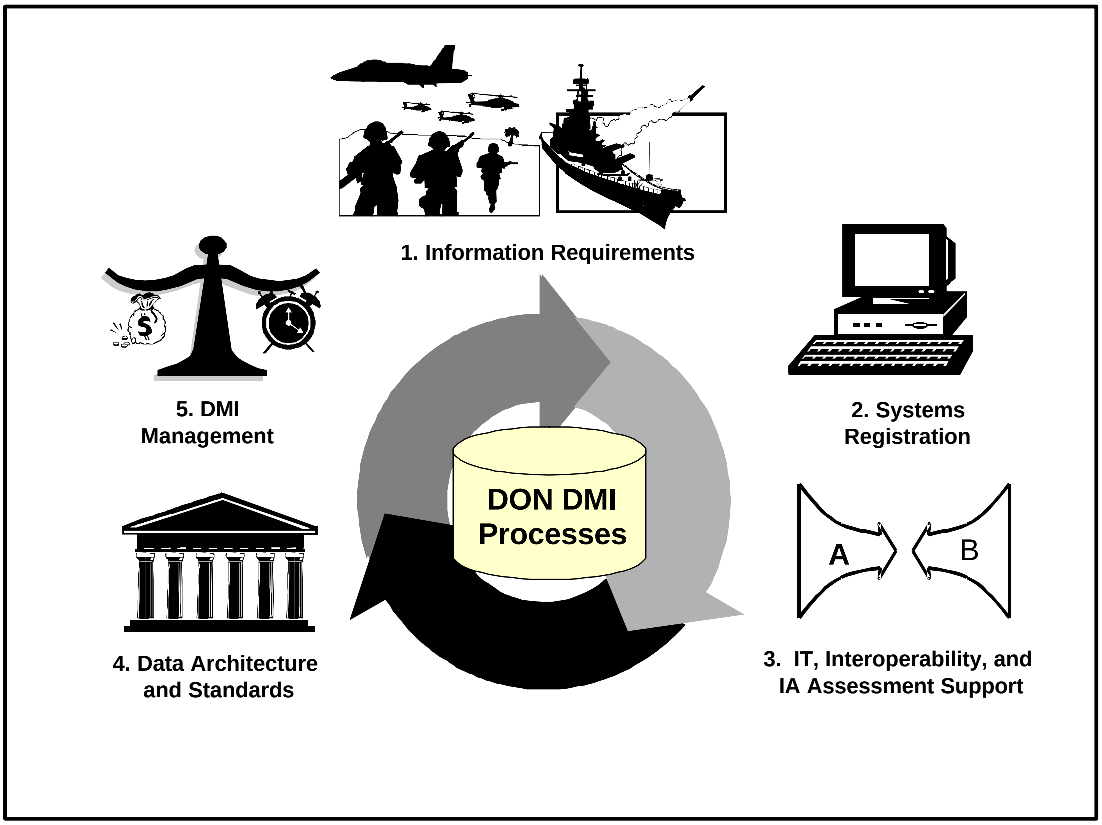

1. Information Requirements
2. Systems Registration
3. IT, Interoperability, and IA Assessment Support
A
B
4. Data Architecture and Standards
5. DMI Management
$
DON DMI Processes

Exhibit 18. DON DMI Concept of Operations

1. The Information Requirements component defines and documents Navy, Marine Corps, and Joint information requirements. They in turn provide focus in the POM for specific problems and/or specific operational capabilities. These subjects are addressed in Sections 2.1.1, 2.2, and 2.3.1.
2. The Systems Registration component includes establishment and maintenance of a system's data requirements baseline, i.e., legacy and new systems/applications database structures and data dictionaries, and systems transfer format implementations documented in a standard or consistent format to provide management visibility. The areas that support systems registration and maintenance are addressed in Sections 2.3.2 and 2.4.

3. The IT, Interoperability, and IA Assessment Support component involves analysis of the systems metadata that is maintained in the DON DMI Repository. This support is addressed in Section 2.7.
4. The Data Architecture and Standards component includes construction and maintenance of DON data models, the designation of Authoritative Data Sources, and the DoD data element standards to support system development and interoperability. These subjects are addressed in Sections 2.5 and 2.6.
5. The Management component involves monitoring systems registration, addressing cross functional interoperability issues, and coordination of efforts to ensure maritime information superiority. Section 2.1 addresses this component.

The additional areas addressed in this section are Training, Outreach and DMI Evaluation.

2.1. Management

Senior leadership commitment is essential to achieve the DON DMI strategic goals. DON DMI is more a management than a technical challenge. Exhibit 19, DON DMI Management Process, shows three levels - the FDM level, the DON level, and the DOD level.

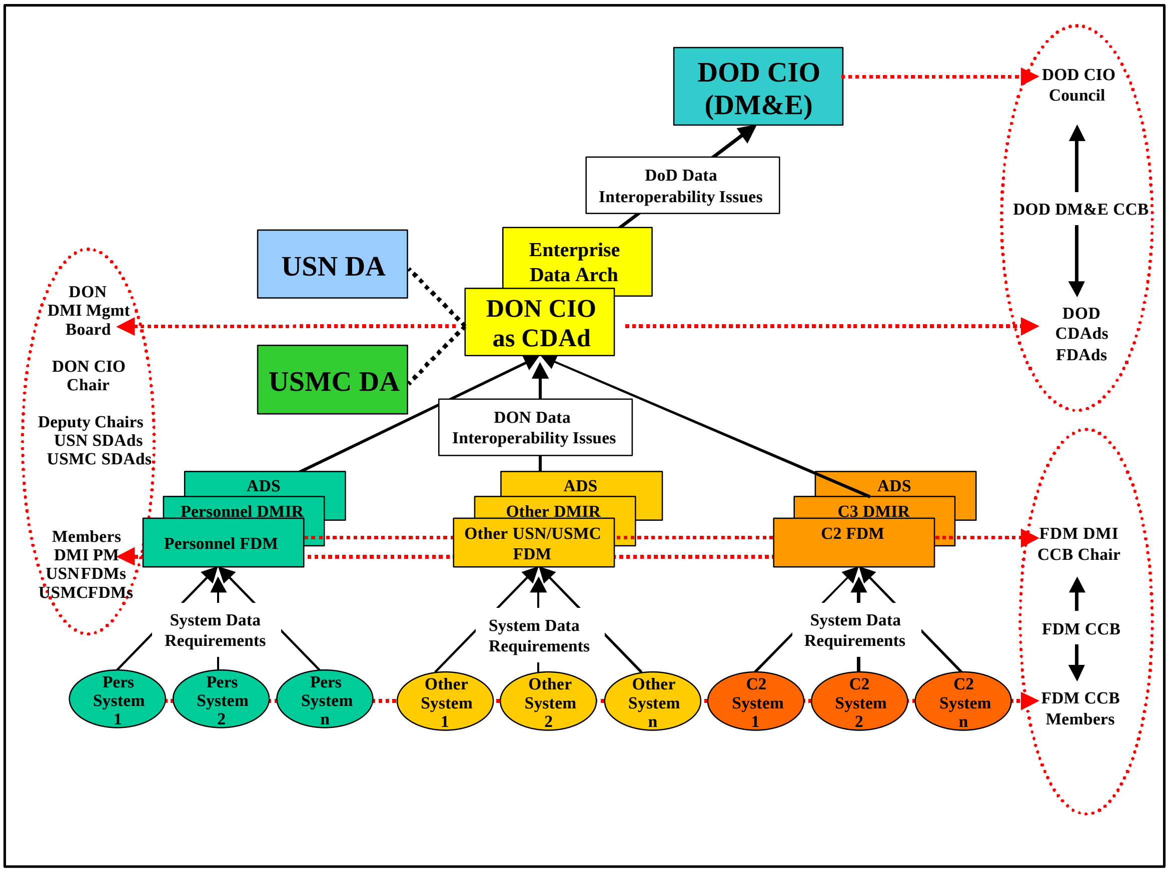


Exhibit 19. DON DMI Management Process

The FDM level involves working with system developers to register their systems and associated metadata and to develop FoS/SoS data architectures and standards. The DON level focus is on implementation and problem solving. The DOD level includes joint requirements definition and coordination.

Significant products to support DMI management include:

- Policy reviews and updates
- Strategic Plan reviews and updates
- Implementation Plan reviews and updates
- DMI Management Board Charter
- DMI Configuration Management Plan
- Program Manager Office (PMO) Charter.

2.1.1. DMI Priorities/POM Guidance

The DMI vision is to have global, affordable and timely access to shared, reliable, and secure data that enables maritime information superiority by 2005. This vision requires identification and prioritization of DMI issues that provide quick term results with a high return on investment. The issues have DON wide impact and directly effect operational performance in support of JV2010 emerging operational concepts. Examples of potential high-payoff data related issues include Unit Identification Code, Combat Identification, and Ship Name.

The DoD directive 4630.5 and instruction 4630.8 define the responsibility for setting information interoperability and supportability requirement priorities within DoD. These requirements and priorities are mapped to system level needs and priorities through architectural analysis. In concert with this analysis, the FDM, with his/her system level view, reflects the hierarchy of requirements and priorities by providing POM guidance to their respective resource sponsor and SDAd. The SDAd brings these requirements to the DON DMI Management Board for approval.

Given this process, the following emerging Joint operational concepts drive the requirement submissions:

- Precision Engagement
- Dominant Maneuver
- Full-Dimensional Projection
- Focused Logistics

2.1.2. Policy

DMI policy as set forth in SECNAVINST 5000.X will be reviewed and maintained by the DON CIO with input from the DMI Management Board and other branches of the Secretariat. In addition, the DON CIO will coordinate with ASN (RDA) on recommended changes to SECNAVINST 5000.2 to ensure acquisition policy reflects DMI requirements as mandated by the Clinger-Cohen Act and DoD directives.

The Service Data Administrators will review and maintain the CNO/CMC Joint Instructions/Orders on DMI and the DMI Joint Implementation Plan. They will coordinate any recommended changes with appropriate Resource Sponsors and FDMs.

2.1.3. DMI Strategic Plan

The DMI Strategic Plan will be reviewed annually and updated as required. Participants will include DON CIO, Service Data Administrators, FDMs and Resource Sponsors as required. Exhibit 20, DMI Planning Framework, depicts the flow of the guiding documents and legislative mandates for the Strategic Plan.

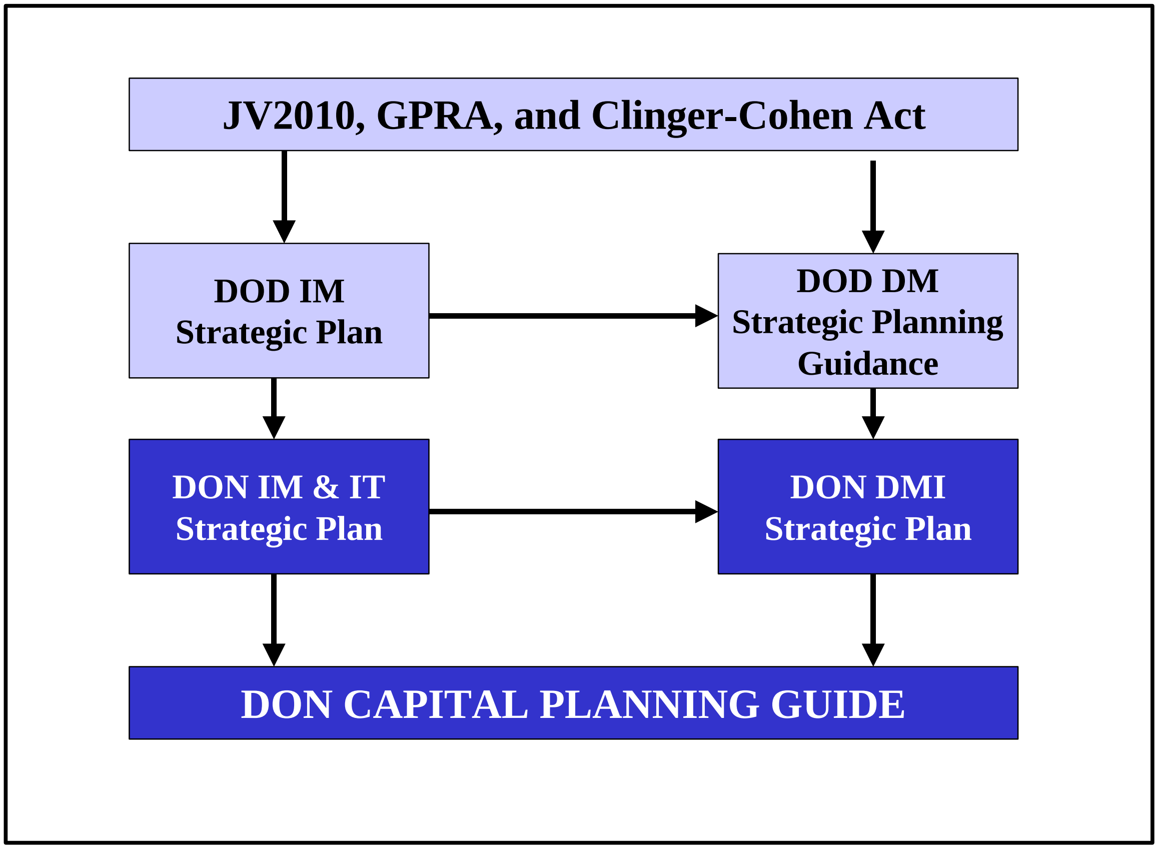

JV2010, GPRA, and Clinger-Cohen Act
DOD IM Strategic Plan
DOD DM Strategic Planning Guidance
DON IM & IT Strategic Plan
DON DMI Strategic Plan
DON CAPITAL PLANNING GUIDE

Exhibit 20. DMI Planning Framework

2.1.4. The DMI Roles and Responsibilities

The DON CIO will charter a DMI Management Board. Exhibit 21, DON DMI Management Roles and Responsibilities, illustrates the overarching configuration management of the DMI from the Functional Data Managers through the DON DMI Management Board to the DoD level.

Roles and Responsibilities	Initiate	Review	Approve	Implement
Management				
Priorities	FDM CCB, DON CIO	SDAds	DMI Mgt Board	DMI Org., Navy&MC Sys. Developers
POM Guidance	SDAds	DON CIO	DMI Mgt Board	DMI Org., Navy&MC Sys. Developers
Policy	DON CIO	DMI Mgt Board	DON CIO	DON
Strategic Plan	SDAds	DMI Mgt Board	DON CIO	DON
Infrastructure (CM)	FDM CCB DMIR CCB	SDAds	DMI Mgt Board	SDAds, FDMs, DMI PMO
PPBS				
Bridge Funding	OPNAV HQMC	CNO, CMC	SECNAV	DON
POM	OPNAV HQMC	CNO, CMC	SECNAV	DON
Acquisition				
MNS/ORDS	OPNAV HQMC	DMI Mgt Board	RDA	System Developers
System Registration	System PMs	FDMs	DMI Mgt Board	
Compliance Testing	System PMs	DMI Mgt Board	RDA	
Repository Implementation				
Pilot Program	DON CIO	DON CIO	DON CIO	DON CIO, FIWC, MARCORPSYSCOM
DMIR Implementation	DMI PMO	SDAds	DMI Mgt Board	FDMs
Configuration Management	DMI PMO FDM CCB	SDAds	DMI Mgt Board	FDMs, DMI PMO
Architecture				
Data Models	FDM CCB	SDAds	DMI Mgt. Board	System Developers, FDMs, Architects

Roles and Responsibilities	Initiate	Review	Approve	Implement
Registration, Reconciliation, and Integration	System Developers, FDMs	SDAds	DMI Mgt. Board	System Developers
Standards Development	FDMs	SDAds	DMI Mgt Board	System Developers, FDMs, Architects
ADS				
Selection	FDMs	DMI Mgt Board	Resource Sponsors	System Developers
Production Requirements	FDMs	DMI Mgt Board	Resource Sponsors	Designated Data Producers
Assessment				
Information Technology	System Developers	DMI Mgt Board	DON CIO	System Developers
Systems Interoperability	Systems Developers, FDMs	DMI Mgt Board	ASN (RDA)	System Developers
Information Assurance	System Developers, FDMs	SDAds	ASN (RDA)	System Developers
Education and Training	SDAs DMI PMO	SDAds	DMI Mgt Board	FDMs, System Developers
Outreach	DON CIO SDAds DMI PMO		DMI Mgt Board	DON
DMI Evaluation	FDMs	SDAds	DMI Mgt. Board	DON

Exhibit 21. DMI Management Roles and Responsibilities

2.2. Planning, Programming and Budgeting System Process (PPBS)

DMI investment must be tied to existing efforts as well as the PPBS. DMI goals and objectives will be tied to the Future Year's Defense Program (FYDP) and Major Force Programs (MFP) to enter the PPBS database. This process is shown in Exhibit 22.

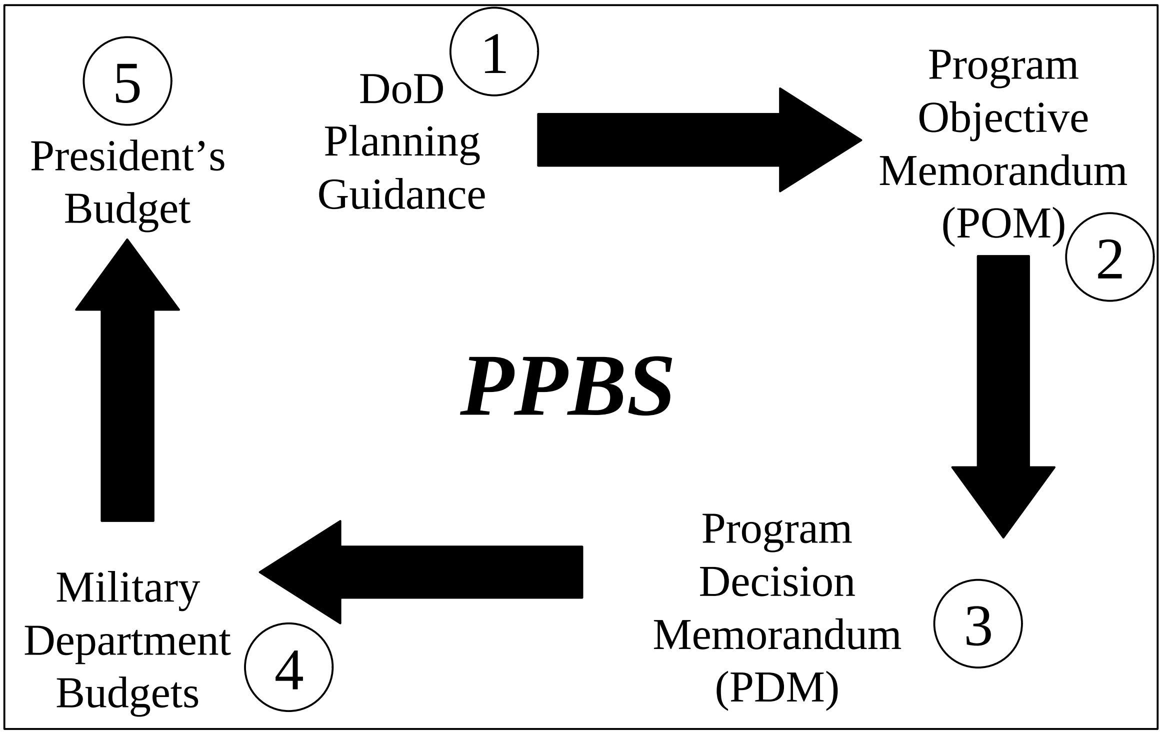

5
President's Budget
DoD Planning Guidance
1
Program Objective Memorandum (POM)
2
PPBS
Military Department Budgets
4
Program Decision Memorandum (PDM)
3

Exhibit 22. Planning, Programming, and Budgeting System Process

The aggressive schedule for DMI Implementation assumes entering the POM process in FY03 and utilizing bridge funding prior to POM inclusion. SECNAV POM Guidance for FY03 will address DMI priorities to solve specific problems, e.g., Authoritative Data Sources, achieve specific operational capabilities, e.g., Combat Identification (CID), Single Integrated Air Picture (SIAP), or to determine data requirements and system data capabilities for emerging joint concepts such as focused logistics. These specific projects will be prioritized by operational and economic factors. In addition, a new or existing Program Element will be used to establish funding for a DMI Program Management Office (PMO).
Significant DMI products to support PPBS include:

- DMI Program Element
- SECNAV POM Guidance
- FDM POM Submissions to their respective Resource Sponsors
- IT budget assessments.

2.2.1. Bridge Funding

To establish Service Data Administrators, Functional Data Managers, PMO, DMI Repository, provide initial training, and initiate identified focus projects, a stabilization fund will be established and be drawn upon to bridge unfunded DMI requirements by the respective Services until the next POM cycle. Each Service is then responsible to POM for the out-years to sustain the materiel solution in the long-term. DON CIO will work with senior managers in the Navy and Marine Corps to identify requisite bridge funding.

2.2.2. Program Objective Memoranda (POM)

DMI funding requirements will be tied to Congressional mandates beginning in POM 03. Based on SECNAV POM guidance, the DON CIO will coordinate with the Service Data Administrators and Resource Sponsors to identify DMI priorities for funding by Resource Sponsors during POM 03 and in subsequent POM and Program Review (PR) submissions. Funding will be required to sustain the DMI organizational infrastructure (Service Data Administrators, PMO, FDMs, Navy and Marine Corp specific Authoritative Data Sources) and the DMI Repository, and to ensure compliance with Congressional mandates and DoD directives in the areas of IT acquisition and interoperability at the data level. DON CIO will review IT budget submissions for compliance with those mandates and directives.

2.3. Acquisition

Certain things need to be done during an IT acquisition to satisfy the requirements of the DON for data management and for interoperability. This section describes how those things should be accomplished.

Significant DMI products to support acquisition include: the DMIR System Registration Template, System Conceptual, Logical and Physical Data Models, System Data Element Dictionaries, Milestone Reviews (I, II, III), Data Standards Conformance/Compliance Testing Reports, Section 8102 Certification, and a revised SECNAVINST 5000.2B to address DMI requirements.

2.3.1. Incorporate DMI Requirements in MNS and ORDs

To ensure interoperability, DMI requirements must be incorporated in Operational Requirement Documents (ORDs), and they must include information interoperability key performance parameters (KPPs).

The ORD contains operational performance requirements for a proposed concept or system. Joint mission area architectures and CRDs provide ORD development guidance through validated performance based overarching capabilities for a given mission area. ORDs translate the Mission Need Statement (MNS) and Capstone Requirements Document (CRD) requirements into detailed, refined performance capabilities and characteristics of the proposed system. ORDs provide the specific requirements base for acquisition and program development.

The focus for the ORD interoperability KPP will be information exchange and required level of information interoperability for the system information needs. The intent is for the warfighter to identify the essential, high level Information Exchange Requirements (IERs) that reflect both the information needs necessary to satisfy the system under consideration and the information this new capability may provide to enhance fielded systems. For ORDs, high-level IERs are defined as those information exchanges that are external to the system, i.e., between nodes. The ORD information interoperability KPP should define the level of interoperability required for the proposed system. Information interoperability KPP will be derived from IERs identified in the mission area integrated architecture and associated CRD that characterize the information exchanges required by the proposed system. ORDs falling under the umbrella of a CRD should ensure compliance with the CRD information interoperability KPP.

2.3.2. Document and Register System and Application Data Requirements and Interfaces in a Common Format

Program Managers or their designated representative will document new and legacy systems/application data requirements in the DMIR using an online systems registration template. This template will be used to record both system data - data about the system required to support acquisition, program, and other interoperability analyses; and associated system's metadata - data about the data required by the system for its optimum performance and data interoperability with other systems.

Program Managers (system registrant) will initiate registration with the Functional Data Manager that corresponds to the functionality of the system being registered starting at Milestone 0 with, as a minimum, the system name and point of contact information. This initial registration provides the FDM, as a DMIR manager, with pertinent information about the system to allow the FDM to establish a DMIR registration account. Once registered, the system registrant will be able to enter either system data or system metadata.

2.3.2.1 Systems/Applications Registration Requirements

A key-based Entity-Relationship Diagram, also known as the conceptual schema or model and sometimes referred to as a data taxonomy or a semantic data model will be registered during Phase 0, Concept Exploration, and is a requirement for Milestone I approval. This model consists of a list of general data areas and a brief description. Example: Medical - those aspects of a person's current state of health and fitness that impact upon his/her readiness to deploy on an operational mission.

Complete registration of the mandatory attributes as provided in the DMI Repository System Registration Forms, Appendix C, for a new system must be completed for Milestone II approval. In addition, new systems also will need to provide a Logical Data Model to promote data re-use across the DON.

It is envisioned that most of the registration will be accomplished in the course of the development and life cycle maintenance phases of a system/application. As changes in the metadata or data structures occur during the life cycle of a system/application, Program Managers will submit updates to the DMIR.

Current contract language does not sufficiently address the requirement for system registration and maintenance. To aid Program Managers, sample language for the Statement of Work (SOW), Contract Data Requirement List (CDRL), and Data Item Description (DID) is provided in Appendices A, B and C.

Existing systems will be registered based on priorities using the IT systems registration database as the basis for determining mission critical systems of record for immediate registration.

2.3.2.2 Milestone Review Requirements

The requirements for Milestone approval are provided in the following table. These requirements are based on DISA recommended products for IT/NSS systems.

Milestone	**Data Perspective**	**Specific Products for Review**
Milestone 0: Approval to conduct concept studies	Constraints, Guidelines and Scope	• Data Administration and Standards Plan that describes how DoD 8320 program will be implemented. • System registration (system name and point of contact as a minimum) with appropriate DON DMI FDMs
Milestone I: Approval to begin a new Acquisition Program	Data Requirements Identification	• Key-based Entity-Relationship Diagram (ERD) in IDEF1X format (also known as the Conceptual Model) • Draft Business Rules • Entity Definitions • Coordination with appropriate FDMs to identify existing entities for use by the system.
Milestone II: Approval to enter Engineering and Manufacturing Development	Data Standards Complete	• Fully attributed Logical Data Model (IDEF1X format with a Data Element Dictionary) registered in DNO DMI Repository (DMIR)

Milestone	Data Perspective	Specific Products for Review
		• Mapping of Business rules to the DoD Data Architecture (DDA) business rules • Coordination with appropriate FDMs for mapping of entities and attributes to Functional Area Metadata Baseline, the DDDS, and the DDA
Milestone III: Production or Fielding/Deployment Approval	Re-Validation	• Review and update in DMIR (as changes occur) of the Logical Data Model and Data Element Dictionary • Registration of the Physical Data Model in the DMIR • Mapping of the Physical to the Logical Data Model

2.3.3. Conduct Conformance Testing

Data standards compliance testing will provide quantitative results concerning a system's data architecture that are indicative of the degree of compliance of the system's metadata to the DoD data standard. The data compliance testing process provides the procedures for analyzing the test requirements, specifying, designing the test, developing an operational process to implement the testing and developing the reporting of test results.

System Test and Evaluation Master Plans (TEMPs) and operational test plans will include at least one critical technical parameter and one operational effectiveness issue for the evaluation of information interoperability. These documents should also specify information interoperability test concepts. The TEMPs should reference and extract requirements from the appropriate MNSs, CRDs, ORDs, C4I Support Plans, and mission area integrated architectures.

The basic data used in the compliance testing are the Logical Data Models for the DoD standard data architecture and the metadata of the information system under test. As a result of testing, a system will have a metric reflecting conformance of its metadata to the DoD standard and a disposition for metadata items of one of the following categories of state: approved, candidate, developmental, archived, and disapproved.

Because of the potential for data standards compliance testing to be burdensome and expensive, compliance testing must be carefully conceived and executed. The testing will be phased in both time and scope. The initial testing will be of a first-order nature, based upon the percentage of agreement with the DoD data standards by the system metadata. As the DMI evolves, additional testing capability will be introduced to evaluate finer grained aspects of data standards compliance.

DMI compliance testing has two components:

- the data standards compliance testing utilizing the system metadata and testing to produce metrics on the completeness, and
- the quality of the description of the system being registered.

The degree of testing related to the system is dependent on the scope of the system data required by the DMIR. The production of equivalently leveled and detailed system descriptive data, such that consistent interoperability assessments can be made, will require careful consideration. This capability is certainly required for those systems with a high potential for interoperability.

The cost of the testing will be reduced by incorporating the initial testing with the system registration. Exhibit 23, Compliance Testing Process Context, presents a notional approach to compliance testing in conjunction with system registration. The submitted system data package is processed to store the system metadata in the DMIR. At that time the metadata will be evaluated against DoD standards and metrics, reflecting the conformance to the standards, will be computed.

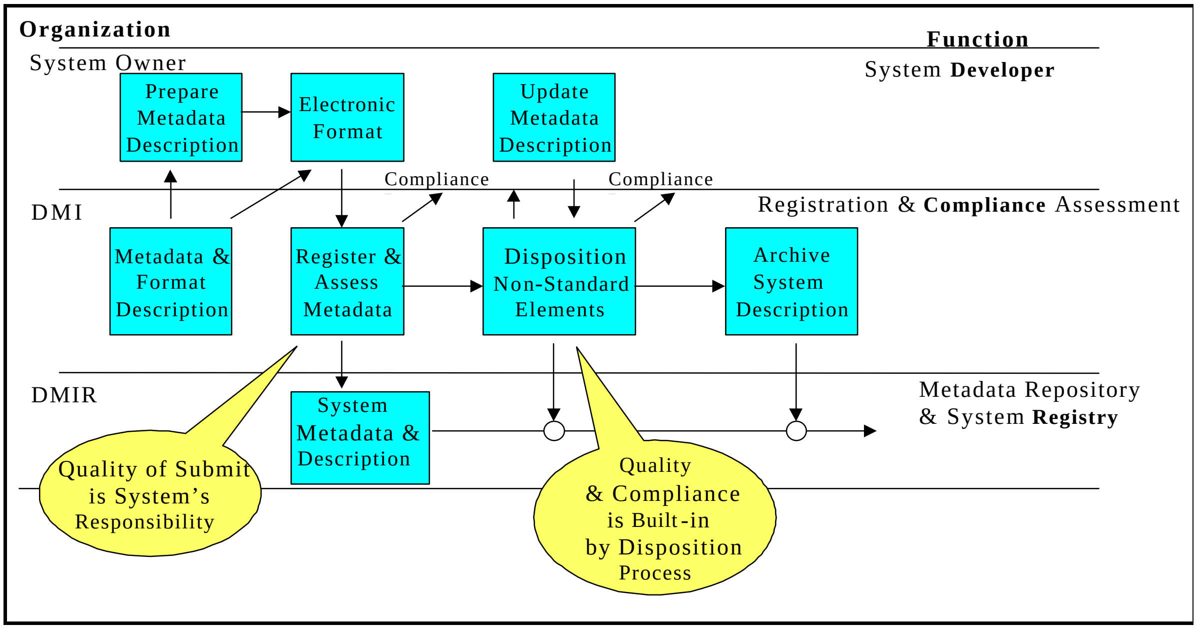

Organization
Function
System Owner
System Developer
Prepare Metadata Description
Electronic Format
Update Metadata Description
Compliance
Compliance
DMI
Registration & Compliance Assessment
Metadata & Format Description
Register & Assess Metadata
Disposition Non-Standard Elements
Archive System Description
DMIR
Metadata Repository & System Registry
System Metadata & Description
Quality of Submit is System's Responsibility
Quality & Compliance is Built-in by Disposition Process

Exhibit 23. Compliance Testing Process Context

The planning for compliance testing starts with the determination of the meaning of compliance, and then the definition of a set of metrics measuring the compliance. This definition of compliance metrics should then be analyzed from the standpoint of phasing into the DMI operations and with respect to interoperability assessment. The resulting roadmap for compliance testing then can be used for planning implementation, achieving an economical set of metrics for initial deployment. The initial set of metrics will then be reviewed for supportability in the development of the software for the registration process. The resulting definition will provide requirements for metrics generation and reporting to the developers of the registration software. The assessment reporting requirements are implemented in conjunction with other DMIR application requirements. The last activity of the test compliance process is to collect all results, including the registration, document the process in a summarized form, distribute and archive the report. The reports are distributed electronically to the recipients. The compliance testing process will be monitored and metrics on the process will be collected to support improvement in the testing process.

Exhibit 24, Registration and Compliance Testing Process Overview, presents an overview of the compliance testing process.

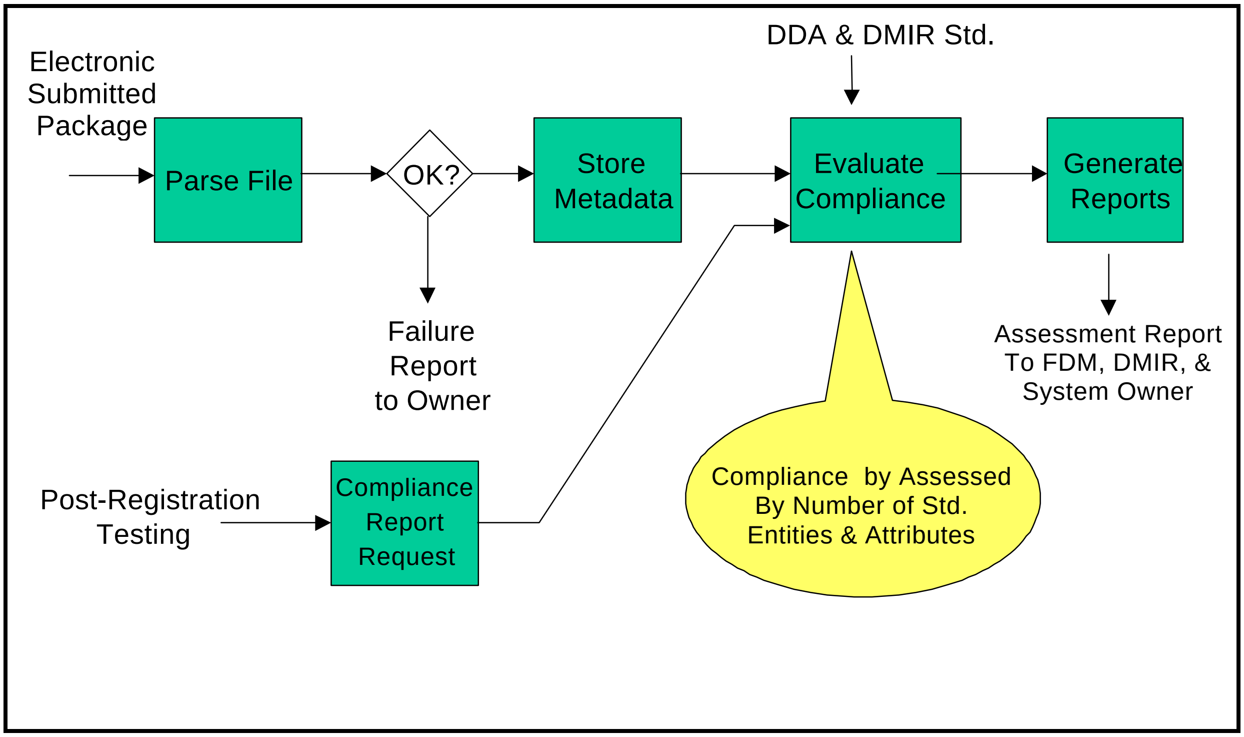

DDA & DMIR Std.
Electronic Submitted Package
Parse File
OK?
Store Metadata
Evaluate Compliance
Generate Reports
Failure Report to Owner
Assessment Report To FDM, DMIR, & System Owner
Post-Registration Testing
Compliance Report Request
Compliance by Assessed By Number of Std. Entities & Attributes

Exhibit 24. Registration and Compliance Testing Process Overview

An accompanying activity will produce material about the conformance testing and its meaning, to be used in other areas of the DMIR, such as orientations, policy interpretations, and training. This will ensure a consistent treatment of the conformance metrics, help build an imperative for data standards conformance through a public knowledge a system's compliance score.

Information systems logical schemas (including relationship verbs), entity, attribute, and domain value names, entity and table compositions (member attributes and fields, respectively), and field sizes and units are compared to the DOD standard data architecture. Metrics are computed and reports are generated based upon the test specification. The actual results are to be compared with the required results and any previous compliance test results to produce comprehensive test results reports. A test conclusion shall be acknowledged according to the previously defined pass/fail decision criteria and documented in the report. The report will provide explanatory text on areas where the system lacks compliance.

2.4. DMI Repository Implementation

The DMI Repository (DMIR) System Requirements Specification discusses the relationship of the DMIR with DMI and the ITA. It provides the DMIR Concept of Operations, requirements analysis for the DMIR, the system design and its functionality, the DMIR logical data model (entity level), and the mandatory entities and attributes required for complete system registration in the DMIR and for Milestone II approval. DMIR implementation across the DON will be phased based on focus areas and funding. The DMIR concept of operations is depicted in Exhibit 25, DON DMI Repository Concept of Operations, and detailed in the Requirements Specification. As depicted, the DMIR will have both NIPRNET and SIPRNET access through a DON portal. It also will contain commercial off the shelf (COTS) and specialized government off the shelf (GOTS) tools for the registration and analysis of system data and metadata.

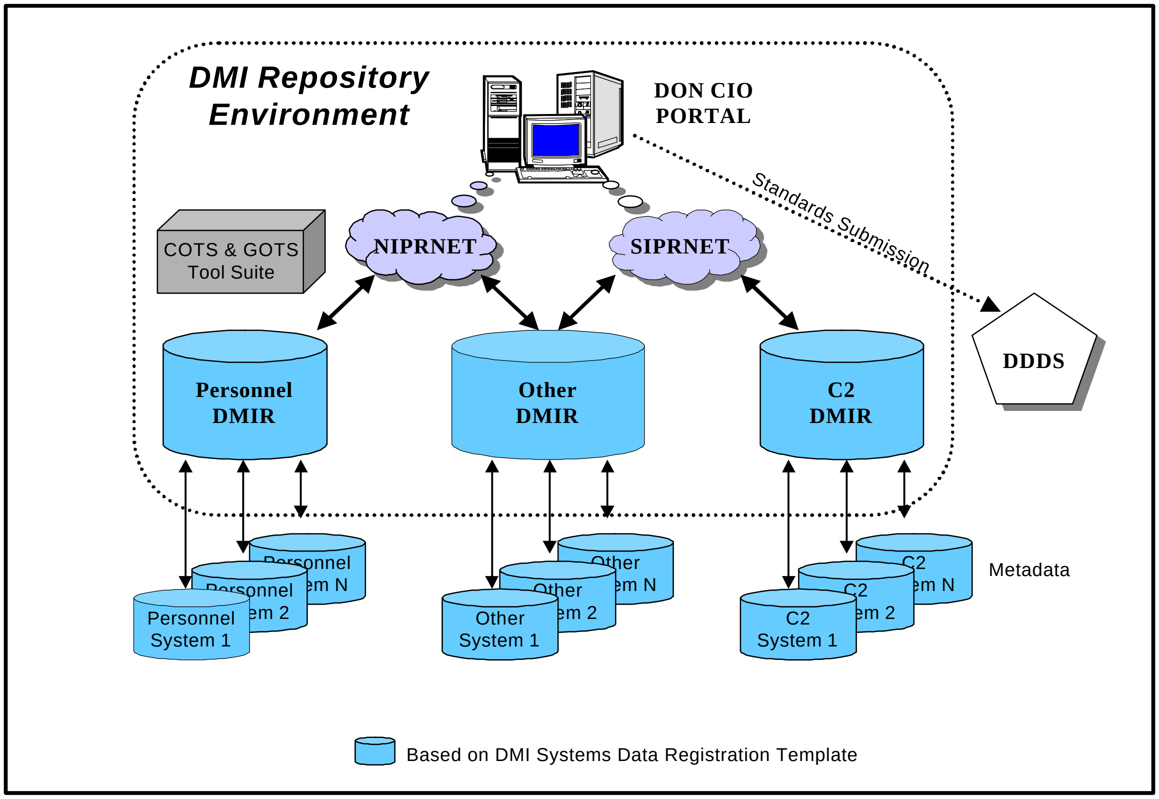


Exhibit 25. DON DMI Repository Concept of Operations

2.4.1. Pilot Program Phase

A pilot program is underway to develop and test portal software, DMIR functionality and FDM implementation procedures. For the pilot program, two functional areas will be connected to the DON portal for testing prior to completing the final design of the DMIR. These areas are Combat Identification hosted at the Fleet Information Warfare Center and a Logistics capability hosted at Marine Corps System Command. Lessons learned during the pilot will be used to solidify the DMIR design and operation.

On successful completion of the pilot it is intended to distribute the DMIR software to the respective FDMs for local use and registration of systems within the respective functional areas. Initial distribution is scheduled for June 2001. As FDMs stand up and focus areas are identified with funding, the DMIR will expand. An initial loading of the DMIR will be accomplished using on the validated data in the DON IT systems database. This will provide a baseline of DON systems from which the respective FDMs can then gather the additional metadata on their systems to develop functional data models as detailed in section 2.5.1.

2.4.2. DMIR Configuration Management

The DMI Repository will have a configuration management board chaired by the DMI PM and whose members will include the FDMs. Exhibit 26, DMI Repository Configuration Management, shows areas of responsibility.

DMIR Configuration Item	MANAGER	PRIMARY USERS	APPROVAL AUTHORITY	STATUS
DMIR Requirements Specification	DMI PM		DON CIO	In progress
DMIR Acquisition NIPRNET Configuration SIPRNET Configuration	DMI PM		MDA and DON CIO	
DMIR Software	DMI PM	FDMs/Sys. PMs	DMI PM	
DMIR Content Items	FDMs	FDMs/Sys. PMs	DMI Management Board	
Training	DMI PM	FDMs/Sys. PMs	SDAds	
Installation Schedule	DMI PM	FDMs	SDAds	
Life Cycle Management	DMI PM	FDMs		
COTS/GOTS Tools	DMI PM	FDMs/Sys. PMs	DON CIO	
Tool Transfer Formats	DMI PM	FDMs/Sys. PMs	DMI PM	
Security	DMI PM	FDMs/Sys. PMs		

Exhibit 26. DMI Repository Configuration Management

2.4.3. DMIR Security

The DMIR, as an information system, must be certified and accredited for use in accordance with existing IA directives. DON CIO, as the Designated Approving Authority (DAA) for the DMIR, will accredit the system during the pilot project implementation. The accreditation process will address the required confidentiality, integrity and availability of services and constraints under which the DMIR can operate including the sensitivity of metadata, domain values and instance data fill, as well as user authorization, physical and system configuration.

Several significant security issues related to DMIR implementation require resolution and will be investigated during the DMIR pilot. These issues include:

- Classification of metadata – In general, metadata is unclassified. However, when domain values and system usage are associated with system metadata, the DMIR can become sensitive but unclassified or classified. The system registration template allows attributes that contain free text as data fill. Detailed instructions will be required to prevent classified information as part of this data fill.
- Sensitive but unclassified metadata - This data must be handled in accordance with privacy and legal regulations as well as security policies.
- Access control and registration policies - Design of the DMIR must address complete registration of systems metadata across the unclassified and classified domains, web access via the .mil domain only, and access by Allied, coalition and NATO partners.
- Data marking - Policy is required for the DMIR to define marking requirements at the record, entity or attribute level. Data marking requires significant data storage overhead and must be considered as a critical system design specification of the DMIR.
- New IT initiatives – NMCI and other new initiatives may provide enhanced security features such as virtual private networks, public key infrastructure and firewall technology, which will impact specific DMIR security issues. The DMIR must be developed and implemented in parallel with these new initiatives.
- Classification of aggregated metadata – No formal guidance or authority currently exists for classification of the aggregation of unclassified systems metadata which, when viewed together, disclose significant system capabilities, vulnerabilities or security related issues. Guidance and adjudication of this issue must be addressed in IA instructions and directives.

2.5. Develop and Manage DON Data Architecture

This section describes five DMI processes, which build and attribute the DON Data Architecture. The DON Data Architecture, as described in Section 1.2.5, is a framework for organizing and managing the inter-relationships of data. This framework contains the optimal design of the data structured and modeled according to DOD data standards guidance. It also contains the specific details regarding the actual implemented structures of data stored and used in operational systems (both legacy and new/migrating systems.) The DON Data Architecture will be developed from top down and the bottom-up. Exhibit 27, Approach for building DON Data Models, below depicts this combined approach.

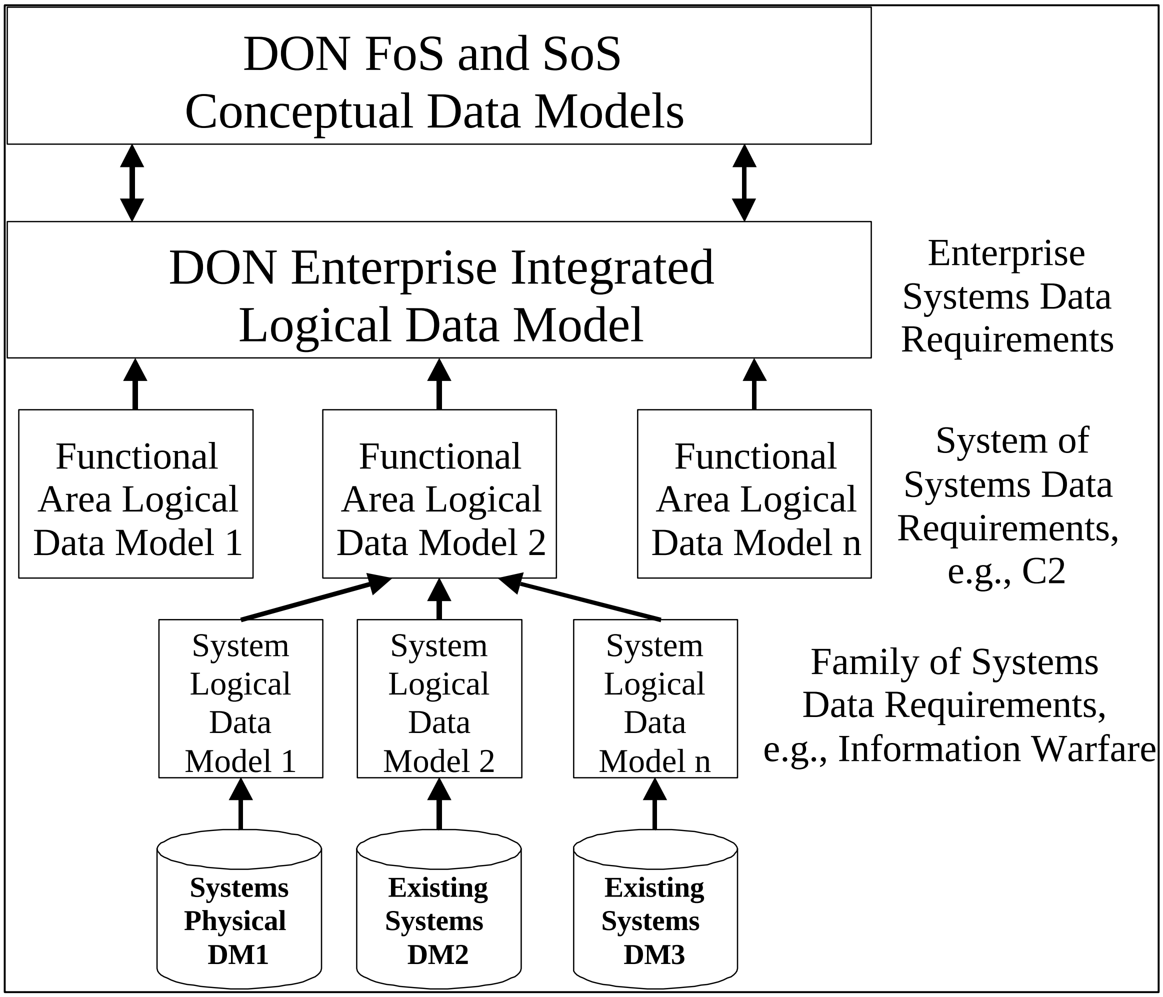

DON FoS and SoS Conceptual Data Models
DON Enterprise Integrated Logical Data Model
Enterprise Systems Data Requirements
Functional Area Logical Data Model 1
Functional Area Logical Data Model 2
Functional Area Logical Data Model n
System of Systems Data Requirements, e.g., C2
System Logical Data Model 1
System Logical Data Model 2
System Logical Data Model n
Family of Systems Data Requirements, e.g., Information Warfare
Systems Physical DM1
Existing Systems DM2
Existing Systems DM3

Exhibit 27. Approach for Building DON Data Models

The top-down approach creates an over-arching, enterprise-wide context of DON’s information requirements (referred to as the DON Enterprise Conceptual Data Model) and is based on all the missions, functions, goals and strategies of the DON’s warfighting and business segments. This conceptual model is also aligned with the DON Data Architecture.

The bottom-up approach utilizes a systems metadata registration process to first capture and baseline existing data requirements as implemented in the operational systems for each DON function. Each system’s data structures are captured as a System Physical Data Model, and are then translated into a System Logical Data Model. Integration of a a functional area’s System Logical Data Models result in deriving a Functional Area Logical Data Model, and cross-functional analysis and reconciliation of the functional area model derives the DON Enterprise Integrated Logical Data Model.

The resultant bottom-up enterprise logical model is then mapped and reconciled to the top-down conceptual model, resulting in validated and aligned top-down conceptual and bottom-up logical enterprise-wide data models for DON. Over time the logical models are further defined and attributed as new systems are designed or existing systems are enhanced or retired.

2.5.1. Develop Enterprise Conceptual Data Model

The approach for building the DON Enterprise Conceptual Data Models is based on a set of technology independent techniques to arrive at a set of high-level conceptual entities that align with the DOD Data Architecture and the CADM. The entities represent the information requirements (at a high-level, super entity view) of DON's warfighting missions and business segments. The identification of the entities are driven by the requirements specified in Capstone Requirement Documents (CRD) for Family of System (FoS) and System of System (SoS) capabilities. Mission Need Statements (MNS) and systems' Operational Requirements Documents (ORD) further define them.

The DON CIO staff, the designated Service DAds and Functional Data Managers will work together as a team in defining and establishing the DON Conceptual Data Model. This team should come together in a focused, facilitated workshop to produce the model. One of the most significant factors of this forum beyond building the enterprise model is building consensus and commitment with the Functional Data Managers towards a DON enterprise view of their data. This becomes critical for future reconciliation's and model integrations as they proceed to define and manage data within their respective functional areas.

2.5.2. Register Systems Data Models

The FDMs will work with their respective system managers to collect and register systems metadata in the DMIR. This process is also described in more detail in Section 2.3.2. System developers will register both legacy and new systems metadata in the DMIR. The system metadata such as table names, data element access names (short name), domain values (range, list of valid values, number or character), element types (character, numeric, float), element lengths, and data security classifications are captured and represent the System Physical Data Model. This instantiation of the data's structure for each system data will vary according to the selected database management system (e.g., Oracle, Sybase) or for optimizing the application's performance.

To enable cross-functional data analysis and standardization assessments, each system's physical data model is translated into a logical model of the data (referred to as the System Logical Data Model). This tranlation involves mapping and matching the system metadata (with synonyms and homonyms) against DoD data standards, recommending the modification of existing standards to meet the systems' requirements, or initiating the development of candidate standards.

Once a number of representative systems are captured and modeled in DMIR and they cover a significant number the functional area entities, the process of developing the Functional Area Logical Data Model can begin.

2.5.3. Develop Functional Area Logical Data Models

The process for developing the Functional Area Logical Data Models starts with each FDM analyzing the System Logical Data Models captured for systems in their functional area. System data (i.e., Data Entities, Data Attributes, and Data Domains) are compared. Data Entities are harmonized by integrating like-entities and like-attributes into common entities. Data Attributes are harmonized by consolidating synonyms (i.e., different attribute names, same or nearly the same definitions and domains) into commonly named attributes with common domains, and by consolidating homonyms (i.e., same attribute names, different definitions and domains) into commonly named attributes with common domains. Entity and attribute naming conventions normally should be consistent with the preponderance of common usage as implemented in the majority of systems registered in the DMIR. The FDM will maintain a mapping of common entity and common attribute names to the synonym and homonym names as implemented in registered systems.

While reconciling the system logical data models, the FDM should engage in a collaborative exchange with system developers to ensure that the resulting common sets of attribute names, definitions, and domains are consistent with the data requirements of all systems in the functional area.

The resultant Functional Area Logical Data Model (with mappings back to the respective legacy systems) can then be used by all systems in the functional area, thereby achieving systems interoperability at the data level within a system of systems (SoS) and family of systems (FoS). These common data entities, attributes, and domains, in turn, will be re-used in support of developmental systems. As legacy systems are retired, the need to map common data to synonyms and homonyms will decrease. Over time mapping will become unnecessary as systems evolve to use interoperable common data.

2.5.4. Develop the DON Enterprise Integrated Logical Data Model

The DMI Management Board will evaluate, compare and resolve any inconsistencies or differences that may exist across the common entities and relationships used in the Functional Area Logical Data Models. Cross-functional consistencies in the logical models as well as conceptual consistency between the logical models and the DON Enterprise Conceptual model is addressed by the board. The DMI Management Board ratifies the final DON Enterprise Integrated Logical Data Model.

2.5.5. Data Standards Development, Submission, Coordination and Validation

This section describes the development, submittal and coordination of new data standards, modifications to existing data standards, and archiving an existing data standard in accordance with DOD 8320.1-M-1; Data Standardization Procedures of April 1998.

System developers should attempt to use applicable external (international, national and federal) data standards before creating or modifying a DoD data standard. FDM's should be consulted to identify existing standards within their functional areas. The DMIR and DoD data dictionaries should also be used to locate adopted external and DoD data standards.

The system developer's objective in developing a logical data model is to model the documented data requirements of a system, and design a data structure that would support those requirements. A data model must include entities and their attributes. Entities and attributes should be named and defined as described in Appendix 5 of the DoD 8320.1-M-1. The logical data model, IDEF1X, should be fully attributed and normalized to third normal form.

New systems require the development of a data model using existing and/or candidate DoD data standards. This development process is iterative. Operational systems will utilize their existing data models. Components of these new or existing data models will be used to create developmental data standards to be submitted for DoD approval as new data standards. Developmental data standards submitted, but not yet approved, are referred to as "candidate" DoD data standards.

For legacy systems, reverse engineering, using a CASE tool, can help produce the needed data models. In many cases it is expected that producing a fully attributed and normalized data model may require extensive effort. System developers should work closely with their FDM's to determine the required level of detail.

This process, which is depicted in Exhibit 28, Data Standards Coordination and Validation Process, addresses coordination of review and consensus of the definition of the non-standard data to proposing this data for DoD approval to.

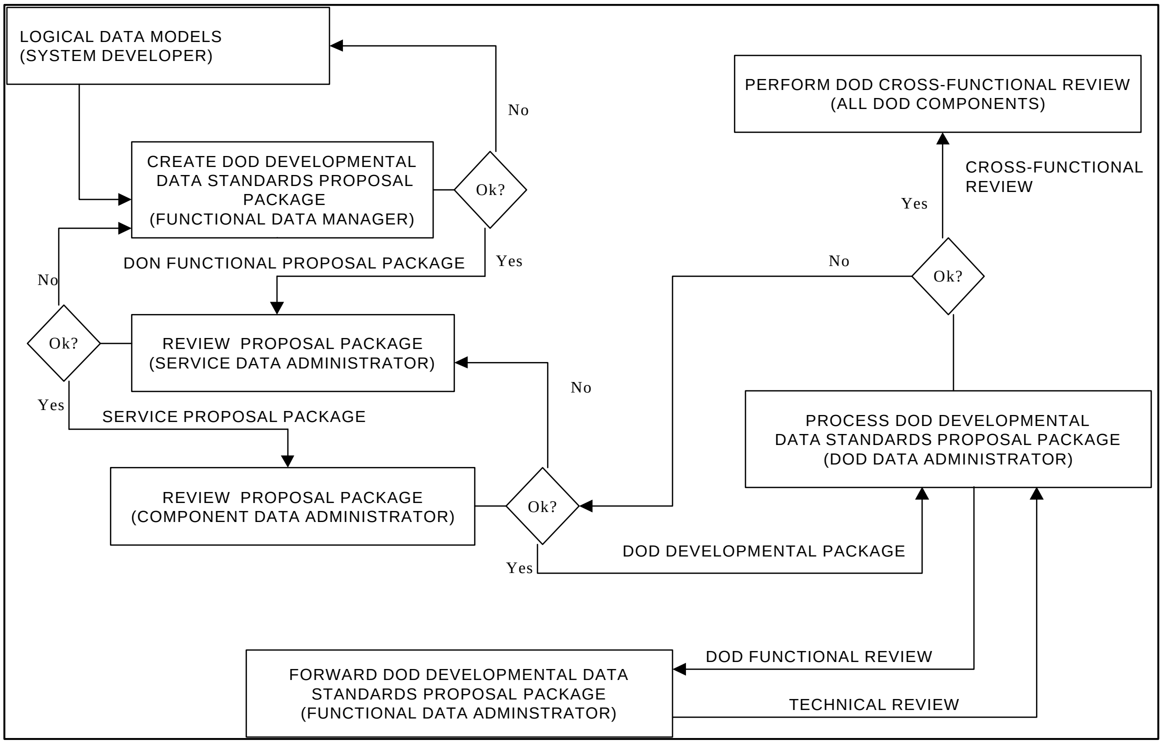

LOGICAL DATA MODELS
(SYSTEM DEVELOPER)
No
CREATE DOD DEVELOPMENTAL DATA STANDARDS PROPOSAL PACKAGE
(FUNCTIONAL DATA MANAGER)
Ok?
Yes
DON FUNCTIONAL PROPOSAL PACKAGE
No
Ok?
REVIEW PROPOSAL PACKAGE
(SERVICE DATA ADMINISTRATOR)
Yes
SERVICE PROPOSAL PACKAGE
No
REVIEW PROPOSAL PACKAGE
(COMPONENT DATA ADMINISTRATOR)
Ok?
Yes
DOD DEVELOPMENTAL PACKAGE
PERFORM DOD CROSS-FUNCTIONAL REVIEW
(ALL DOD COMPONENTS)
CROSS-FUNCTIONAL REVIEW
Yes
No
Ok?
PROCESS DOD DEVELOPMENTAL DATA STANDARDS PROPOSAL PACKAGE
(DOD DATA ADMINISTRATOR)
FORWARD DOD DEVELOPMENTAL DATA STANDARDS PROPOSAL PACKAGE
(FUNCTIONAL DATA ADMINSTRATOR)
DOD FUNCTIONAL REVIEW
TECHNICAL REVIEW

Exhibit 28. Data Standards Coordination and Validation Process

This process begins with the submission of a “finalized logical data model” to the FDM from the systems developer. A “standards compliance assessment”, a list of “mapped and matched metadata”, and the “non-standard data requirement(s)” will be produced by the FDM using the DMIR. If needed, the systems developer may be asked for additional information or to modify the data model. A “data standards proposal package” containing “developmental data standards” derived from the list of “nonstandard data requirements” will be reviewed by the FDM to determine the cross-functional impact of the non-standard metadata. The FDM will then proceed with the standardization process or direct the system developer to make modifications to or disapprove the proposal. If appropriate to proceed, the FDM will certify that the package is consistent with DMIR/DDDS and DoD 8320.1-M-1 in terms of Data Model, Entities, Data Elements, and Domain Values, package content, etc. The FDM will then forward the developmental proposal package with its certification to the SDAd who will determine to proceed with the standardization process, return the package for further development, or disapprove the entire proposal package.

2.5.5.2 Coordinate Developmental Data Standards Across the Functional Area

A preliminary review is conducted within the functional community to coordinate the developmental data standards. This is an iterative process that requires the participation of the originator, SMEs, FDMs and joint counterparts. Data originating in support of a DoD functional requirement should be coordinated with the appropriate FDAd.

Prior to placing a proposed modification to an approved DoD data standard, the model originator will coordinate the proposed change with the affected system program managers that are registered as users of the approved DoD data standards and joint counterparts. This coordination will enable system program managers and joint counterparts to measure the impact of the proposed modifications on existing systems that use the data. The FDM will decide whether to forward the proposed data standard change proposal package based on an assessment of the submitting systems status and its level of standards compliance and impact across the functional area. The FDM may also decide to disapprove the change or send the change back to the system developer for further modification.

2.5.5.3 Coordinate Developmental Data Standards Across the Service

The SDAd will perform a preliminary review of the level of standards compliance and the status of the system submitting the metadata. This is a high-level determination of whether a system is new, migrating or legacy and whether or not the proposed DoD developmental data standard(s) are required. A review of the compliance assessment results is fed back to FDM and systems developer.

The SDAd will decide whether to forward the data standards proposal package based on the above review and its impact across the service. If the proposal package is appropriate, the SDAd will certify the package and forward it to the CDAd. The SDAd may also decide to send the package back to the FDM for further modification or disapprove the entire proposal package.

2.5.5.4 Coordinate Developmental Data Standards Across the Component

The CDAd will review the data standards proposal package, the SDAd certification, and the impact across the services. If appropriate, the CDAd will certify that the package is consistent with DMI policy and procedures and forward the DoD developmental data standards proposal package to the appropriate FDAd. The CDAd may also decide to send the package back to the SDAd for further modification or disapprove the whole package.

2.5.5.5 Coordinate Developmental Data Standards Across the DoD

After the FDAd reviews the proposal functionally, the FDAd will either inform the DODDAd that the proposal is appropriate for formal DoD cross-functional review or return the proposal to the CDAd requesting modification. The DODDAd will perform a technical review. If the technical review is approved, the proposed data standard(s) will be changed to "candidate" status and the proposal package will be distributed for the formal DoD cross-functional review. The cross-functional review is normally 30 calendar days and goes to all DoD components, organizationally and functionally. If the technical review is not approved, the DODDAd will return the proposal package to the CDAd with justification as to why the package was not approved for cross-functional review. If the proposal is approved, the candidate DoD data standards will become approved DoD data standards and the logical data models should be modified to reflect that the data is now standard.

2.5.5.6 Manage Cross-Functional Review

The cognizant SDAd and FDM will resolve DoD cross-functional review issues/conflicts with DODDAd and the appropriate FDAd and negotiate settlement through consensus. The SDAd will then forward corrections to the DoDDAd and direct the FDM to update the DMIR.

2.5.5.7 Disseminate Approval/Disapproval Status

At the completion of the DoD data standards approval process, the SDAd will notify the FDM of data standards disposition via the DoD Standardization Report and will direct the FDM to update the DMIR with the new status. Notification and direction will occur within 10 workdays after completion of the DoD approval process. The FDM will disseminate the status to lower echelons and determine subsequent efforts if data standards are disapproved. The DoD Standardization process is complete when the DMIR is updated with the final data standard results and the DON FDMs are notified of the data standard disposition.

2.6. Authoritative Data Sources

Section 1.2.6 discussed the need for Authoritative Data Sources (ADS). This section provides guidance on their selection of ADSs (databases) and the role of ADS Producers in responding to taking by Resource Sponsors for the required instance data.

2.6.1. ADS Selection Criteria

As specified in SECNAVINST 5000.X, Functional Data Managers (FDMs) are appointed by their respective resource sponsors. To support DMI within their respective functional (domain) areas, the FDMs are charged to identify Navy and/or Marine Corps ADS for common mission requirements. The FDMs are responsible for the metadata associated with their functional area assignments. In some cases, they also may be an Authoritative Data Source Producer, e.g., Fleet Information Warfare Center for Navy Electronic Warfare parametric data. In both cases, FDMs will need to work closely with System Developers in their respective functional areas to ensure they understand the needs of the system/application in terms of the data granularity and update cycle required by the system/application. The following criteria will guide ADS selection and designation.

- Where mutually common functional areas exist between the Navy and Marine Corps (e.g., weather, intelligence), the Navy or Marine Corps resource sponsor supporting the preponderance of systems within that functional area will designate the FDM for that functional area and corresponding ADS to be used within that functional area by both Navy and Marine Corps systems/developers. Where functional areas are common, but not mutually so (e.g., Marine Corps personnel systems versus Navy Personnel Systems), each Navy and Marine Corps resource sponsor will designate Service FDMs who will designate the ADS appropriate for that service's functional area requirements.
- A single ADS (database) will be designated as the specific source for functional reference data within a specific functional area, e.g., MIDB for Order of Battle information. This recognizes that there are often technical differences between data that may otherwise appear to be identical. For example, finished intelligence data is the result of a data fusion process that combines the raw data from multiple intelligence disciplines (e.g., communications and non-communications sensor data). In such cases it is appropriate to designate a single ADS for Finished Intelligence, a single ADS for Communications Sensors Data, and a single ADS for Non-Communications Sensors Data. The same is true in situations where data is "streaming" such as direct active sensor input such as from Radar to a tactical link. In this case the ADS would be the live data on the link.
- First priority for ADS designation will be those Navy and/or Marine Corps databases produced by organizations currently officially designated by their resource sponsor and codified in existing Missions, Functions, and Tasks Instructions which define the producer agency's charter, or other appropriate instruction. For purposes of this guidance, an "appropriate instruction" is considered to be an effective DoD Directive (when specifically applicable to a Navy/Marine Corps ADS Producer), SECNAVINST, OPNAVINST, or Marine Corp Order. Examples of currently recognized ADS producers are the Office of Naval Intelligence (ONI), producer of Naval Maritime Intelligence Data, and the Naval Meteorology and Oceanographic Command (METOC), producer of authoritative meteorological and atmospheric information. Both of these ADS producers can cite appropriate instructions as their charter for ADS production. In cases such as these the FDMs only reaffirms the ADS designation.
- ADS designation for each "Table" of the FDM's overarching functional database architecture should be based upon mission and specific system/application requirements

in terms of data granularity.A single source at the Table level is desired because arbitrarily combining ADSs for this level of structure or lower (e.g., data elements) has the potential of creating an inaccurate hybrid view of the Entity at the Table Level because the multiple sources have provided 1) disparate and/or non-synchronized representations of the data instance, or 2) representations of the instance based on sources of varying quality (e.g., finished intelligence versus raw sensor data).

- No database produced below Tier 3, as illustrated in Exhibit 15, Reference Data Cascading, should be designated as a Service ADS.

ADS Reference Data Selection Hierarchy

- National Agencies, e.g., Department of Commerce (Country Codes), State Dept (Diplomatic List), etc.
- DoD Agencies/Producers, e.g., DIA (MIDB), NSA (Kilting, EPL)
- Joint Approved Production Centers, e.g., DIA – MIDB for General Military Information
- Service specific data, e.g., FIWC (NERF for Navy EW)
- Theater-wide application, e.g., CINCPACFLT deployment schedules
- Mission specific live feeds, e.g., Link 16

ADS Designation Process

- Determine appropriate level of data selection (see above – use the highest level most appropriate based on system user requirements)
- Coordinate with production authority in terms of periodicity needed by worst case system
- Promulgate ADS via email and posting in DON CIO DMIR
- Solicit feedback from operational users as to quality of data

Selection of appropriate ADS is illustrated in Exhibit 29, The ADS Selection Process. As new or legacy systems/applications are identified, the metadata registration process begins with minimum entry of the system name and point of contact into the DMIR. Section 2.3.2.1, Systems/Applications Registration Requirements, describes the registration process. Based on the nature of the registered metadata, an ADS designation might be apparent. In this case, the ADS is designated and registered in the DMIR for the system/application. If the ADS is not easily identified, the system/application should be mapped to existing functional areas to determine the applicable ADS. If the functional area source is not known, the CDAd will identify an existing functional area for the system/application through the DMI Management Process illustrated in Exhibit 19. After a functional area source is identified, the FDM can review the registered ADS and designate and register the appropriate ADS for the system/application. If registered ADS do not support the system/application, the FDM will use the DMI Management Process to resolve the ADS issue.

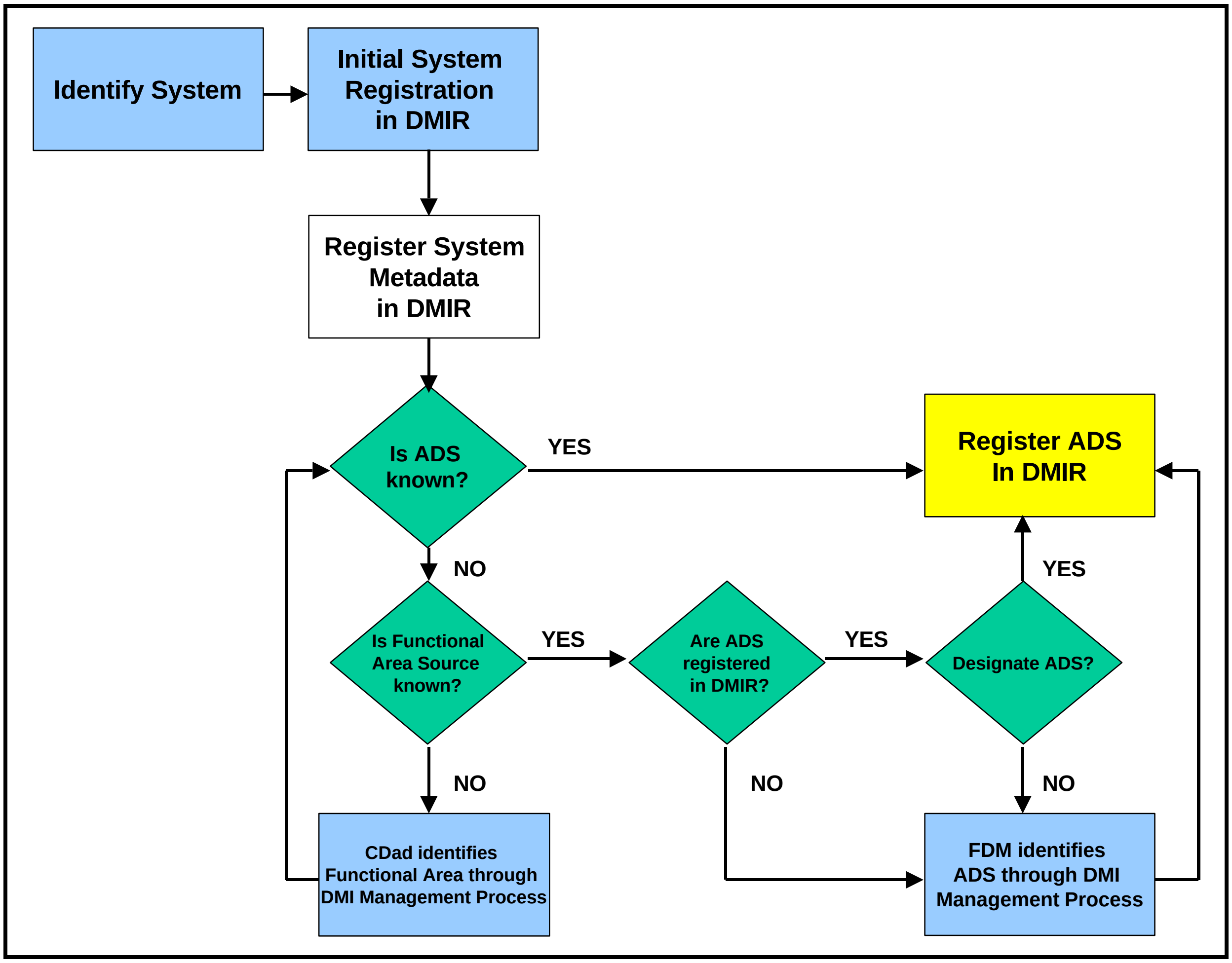

Identify System
Initial System Registration in DMIR
Register System Metadata in DMIR
Is ADS known?
YES
NO
Register ADS In DMIR
Is Functional Area Source known?
YES
Are ADS registered in DMIR?
YES
Designate ADS?
YES
NO
NO
NO
CDad identifies Functional Area through DMI Management Process
FDM identifies ADS through DMI Management Process

Exhibit 29. The ADS Selection Process

FDMs should consider the following points when designating ADS.

- Determine the appropriate level of data source selection based on the ADS Reference Data Selection Hierarchy shown above.
- Coordinate with production authorities in terms of periodicity needed by worst case system data requirements.
- Promulgate ADS selection via email and registration in the DMIR.
- Solicit feedback from operational users as to the quality of data.

As the FDMs designate the different ADS for their areas of responsibility, they may determine that there are not currently any existing sources of data for the different requirements identified by system developers. The FDM, in conjunction with the System Developer, will identify this shortfall to the resource sponsor, who in turn will identify and fund appropriate production centers or facilities to satisfy the data shortfall.

The FDM will maintain a list of the ADS/POC information for each system/application registered in the DMIR. This list will be made available to system developers and users via the DMIR. Additionally, FDMs will provide ADS listings to their appropriate CNO/CMC sponsors. CNO/CMC will inform system developers of the FDMs to contact during their system and application development for information on ADS.

2.6.2. Roles of ADS Producer

In exercising management of the functional area DMIR, the FDM is able to precisely map requirements for instance data production to the data requirements of the systems registered into the functional area baseline of supported systems. As illustrated in Exhibit 30, ADS Producer Tasking, where this Resource Sponsor-FDM-ADS relationship exists, the resource sponsor may authorize direct liaison authority between the FDM and the ADS producer for purposes of instance data production tasking. In so doing, the resource sponsor is assured production requirements in all instances equals, and will be more responsive to, the actual data requirements of supported systems. Accordingly, as new systems are registered and old systems are retired, instance data production tasking is continuously being adjusted to efficiently align to actual requirements. This will result in the more efficient employment of production resources and provision of more complete and comprehensive data to supported systems. Where the Resource Sponsor-FDM-ADS relationship does not exist, the FDM should forward requirements for instance data production to the Resource Sponsor of the respective ADS for action.

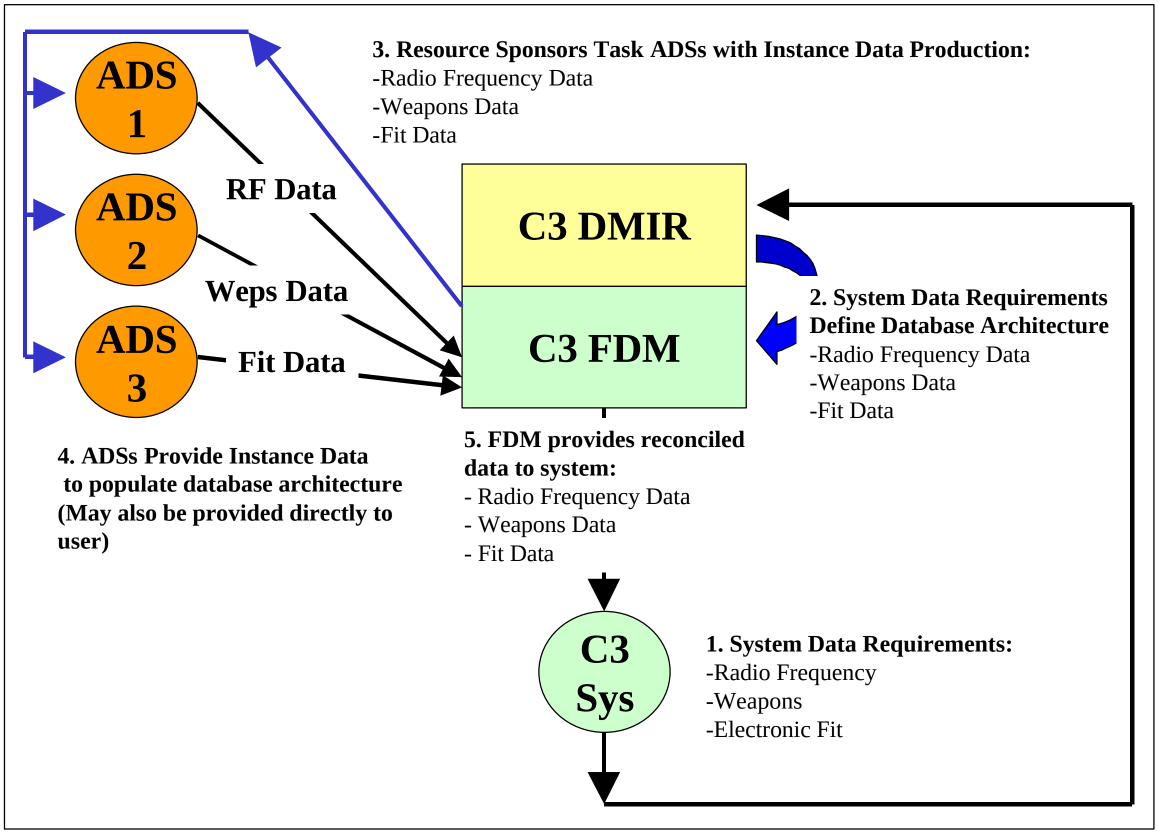

ADS 1
ADS 2
ADS 3
RF Data
Weps Data
Fit Data
3. Resource Sponsors Task ADSs with Instance Data Production:
-Radio Frequency Data
-Weapons Data
-Fit Data
C3 DMIR
C3 FDM
2. System Data Requirements Define Database Architecture
-Radio Frequency Data
-Weapons Data
-Fit Data
4. ADSs Provide Instance Data to populate database architecture (May also be provided directly to user)
5. FDM provides reconciled data to system:
- Radio Frequency Data
- Weapons Data
- Fit Data
C3 Sys
1. System Data Requirements:
-Radio Frequency
-Weapons
-Electronic Fit

Exhibit 30. ADS Producer Tasking

2.7. Assessment Support

DMI assessment support addresses the areas of systems interoperability, the data component of IT, and information assurance. Analysis of systems metadata stored in the DMIR will enable these assessments.

Significant DMI products to support the respective assessments include:

- IT: number of tables and data elements by functional and mission area, number of tables and data elements reduced through integration/consolidation, ratio of standard to non-standard data elements within each system, number of unique system interfaces, number of unique system interfaces reduced through application of standards.
- Systems Interoperability: database to database comparisons at the table and data element level, data elements to transfer format fields (OTG, MTF, XML and TADIL), number of synonyms and homonyms within a functional area and across the Enterprise.
- Information Assurance: comparisons of a system's master metadata file to the physical instantiation of the metadata.

2.7.1. Information Technology Assessment Support

The assessment of DON IT systems can be achieved by a combination of mutually supporting DoD and DON processes. First, the OSD has established Guidance and Policy (G&P) for DoD Portfolio Management and Oversight, from which DON IT Investment Portfolio guidance has been developed. Secondly, the DMIR collects DON IT Systems metadata which can support decision/analysis of performance improvement or cost savings (i.e., re-use of data segments/data elements); relevancy to mission (i.e., mapping data to mission requirements) and risk. Issues which may arise from assessments of IT investment portfolios will be addressed by the DMI Management Board.

The core concepts of the OSD G&P memo on Portfolio Management and Oversight specify the following criteria. Selections must be based up decisions that:

- show measurable improvements in goals and outcomes,
- support the capability of the warfighter,
- support interoperability and Information Assurance,
- support Clinger-Cohen Act, and
- include stakeholder participation.

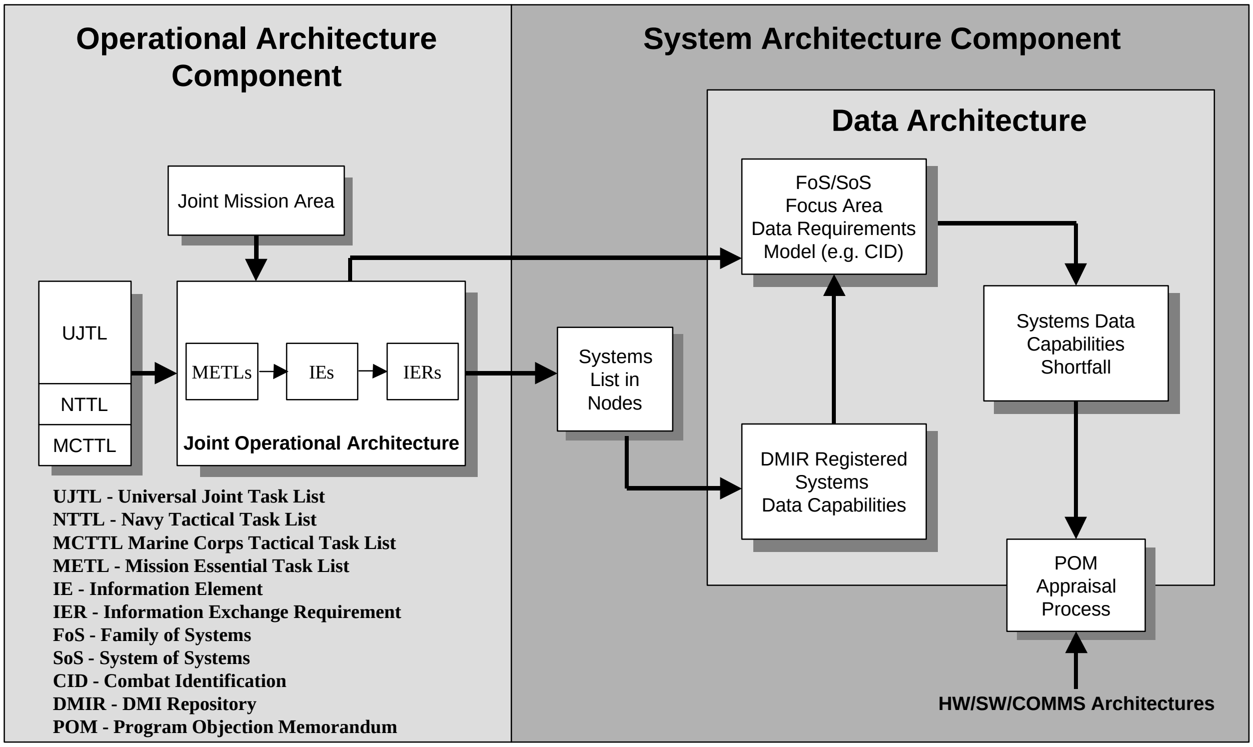

Operational Architecture Component
System Architecture Component
Data Architecture
Joint Mission Area
UJTL
NTTL
MCTTL
METLs
IEs
IERs
Joint Operational Architecture
Systems List in Nodes
FoS/SoS Focus Area Data Requirements Model (e.g. CID)
DMIR Registered Systems Data Capabilities
Systems Data Capabilities Shortfall
POM Appraisal Process
HW/SW/COMMS Architectures
UJTL - Universal Joint Task List
NTTL - Navy Tactical Task List
MCTTL Marine Corps Tactical Task List
METL - Mission Essential Task List
IE - Information Element
IER - Information Exchange Requirement
FoS - Family of Systems
SoS - System of Systems
CID - Combat Identification
DMIR - DMI Repository
POM - Program Objection Memorandum

Exhibit 31. IT Assessment Support

As depicted in Exhibit 31, IT Assessment Support, mission information requirements are determined through the Operational Architecture process. The identified information elements (IEs) for a mission area (generic or specific) provide the basis for developing a data requirements model. The Information Exchange Requirements (IERs) identify the nodes that will send and receive information to satisfy mission requirements. These nodes in turn either have existing systems in place to receive, process and disseminate the information or they will require additional system capabilities. Using a listing of current systems in the respective nodes enables analysts to extract information from the DMI Repository on registered systems data capabilities. This metadata is used to detail or attribute the data requirements model. The attribution can be done either from a family of systems or system of systems viewpoint depending on the scope of the mission area requirement. If current systems capabilities satisfy all the data requirements, then there is no shortfall and no requirement for additional system data capabilities. If on the other hand, there are data requirements that are not satisfied by current capabilities, then there is a shortfall in capabilities that is entered into the POM appraisal process for prioritization and funding. This approach also provides a direct mapping of mission information requirements to specific systems in direct support of Clinger-Cohen Act.

The Portfolio Analysis of Alternatives (AOA) also can be used to identify capabilities and trade-offs. Analysis criteria should be based on Operations Analysis (i.e. those criteria which meet mission performance metrics, minimize total cost of ownership and provide best value options) or Post Deployment Review (i.e., the fulfillment of projected contributions to the organizations mission).

Incorporating the guidance provided in the DON IT Portfolio Memorandum, the G&P PMO Memorandum, and the DON IM/IT Goals, the choice(s) resulting from the resolution of IT portfolio assessment issues should be based upon

- evaluation which measures the contribution to mission goals
- products which ensure mission process and IT become even more agile and aligned, and
- proposals which optimize IT capabilities

The mandated IT assessment activities are external to the DMI, per se, and can only be indirectly supported by the DMI. The resolution of metadata-related issues will be facilitated by developing data queries and reporting capabilities for the DMIR data. These standard capabilities, in addition to ad hoc queries and reports, will enable the DMI staff to support the assessments.

2.7.2. Systems Interoperability Assessment Support

As shown in Exhibit 32, system to system data interoperability is comprised of many aspects. DMI and the DMIR address only the entities, attributes and values of systems/applications data requirements and the transfer formats they use to convey data from one automated system to another. In addition to the data and transfer formats, software interfaces and hardware configurations are also important and must be in synch for interoperability.

The reconciliation process described in Section 2.5.3 will ensure all classes of systems within a Functional Area are mapped to common names, definitions and values in the logical data model. This mapping will provide the metadata baseline for systems interoperability assessments by operational forces. However, the actual physical implementations (versions in use and modifications) of the systems and transfer formats used by individual systems on ships, aircraft, submarines or shore establishments will need to be compared to ensure that they can interoperate at the data level.

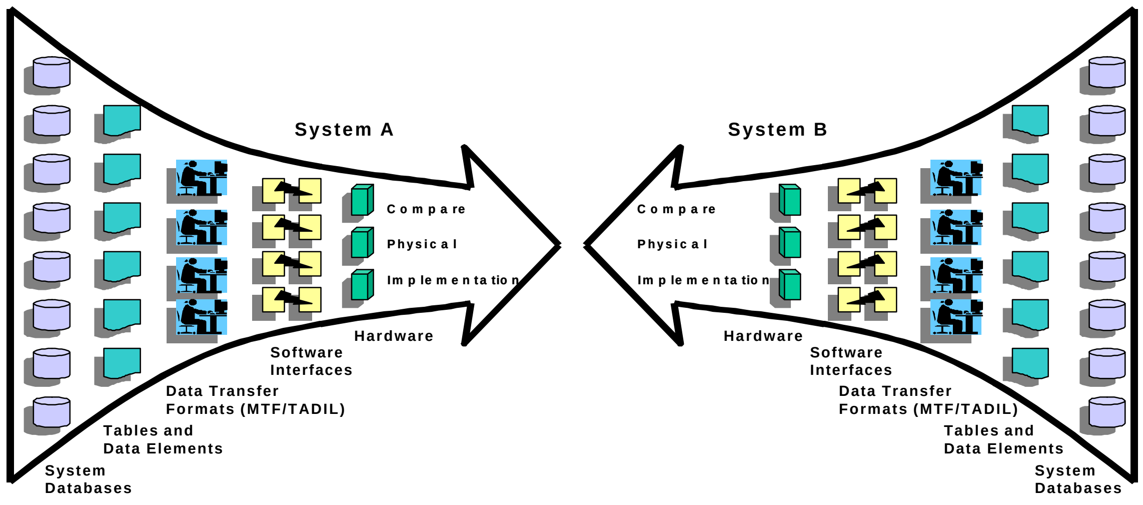


Exhibit 32. System to System Data Interoperability Assessment

2.7.3. Information Assurance Assessment Support

Data integrity is an essential element of information assurance. Just as instance data can be changed to provide incorrect answers, so too can metadata be changed to mislead. The adage is simply you can not protect what you do not know you have. Metadata documentation to the domain level is critical for information assurance. As depicted in Exhibit 33, Information Assurance Assessment Support, routine matchings of master metadata holdings for systems against the physical instantiations of those systems provides the means to assure that the physical system has not been modified except as authorized. The DMIR will contain tools to assist in metadata comparisons.

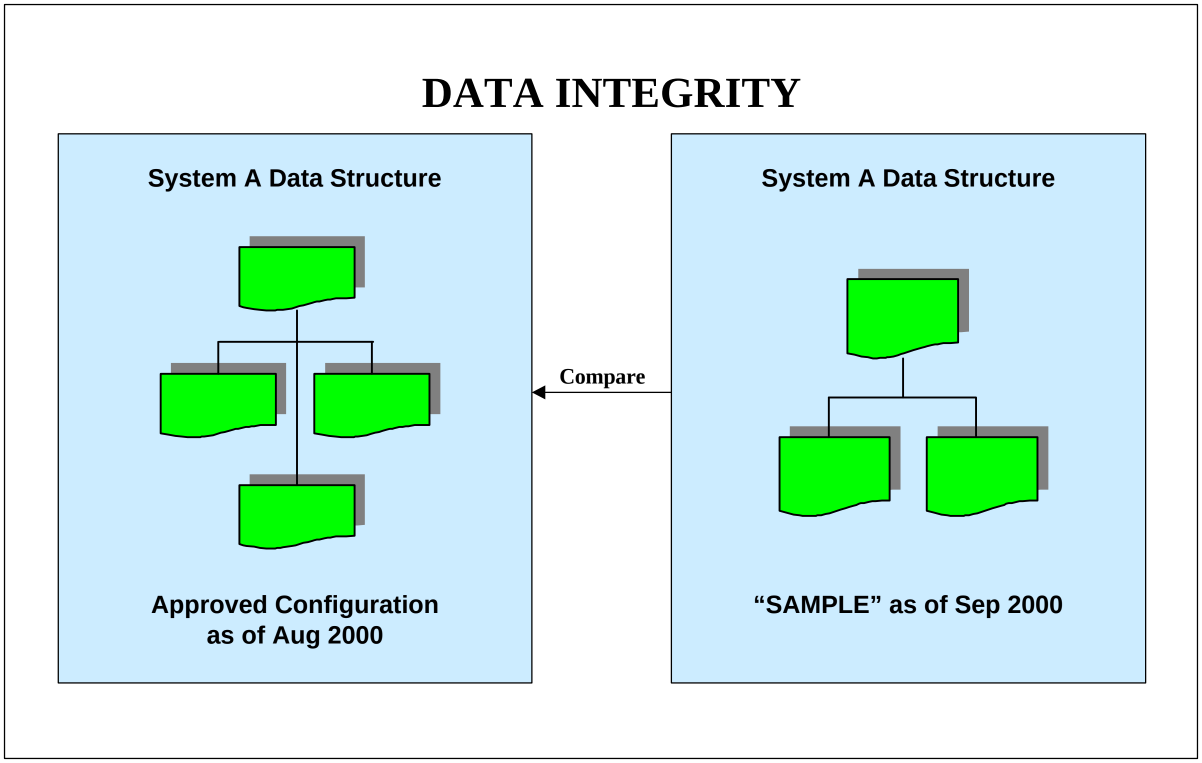


Exhibit 33. Information Assurance Assessment Support

2.8. Training

Information Management/Information Technology (IM/IT) education and training is fundamental to supporting an Information Age. Beginning at the entry level, education and training is required to ensure that professional competencies are maintained at all levels of the infrastructure, i.e., from each organization’s Chief Information Officer (CIO) to the end-user.

The Service Data Administrators and the DMI Program Office are responsible for the development of content specifications and each organization for development of individual training requirements for personnel.

The DMI Program Office in conjunction with the Service Data Administrators will identify core capabilities and user training needs as well as implement and sustain capabilities and training.

Each organization's Strategic Plan should include a specific goal that includes a requirement to achieve IM/IT competencies for its staff. Organizations should identify those personnel required to achieve a competency, and ensure that each person's Individual Development Plans (IDP) includes the appropriate training in accordance with the Service Data Administrator Training Plan. The organization should immediately begin enrolling their staff in the appropriate training.

Each Service Data Administrator will develop a training plan for their respective Service. This plan will include the identification of who should receive training, the level of training needed to support the appropriate level of competency, and what delivery method might be employed.

The DON population comprises three IM/IT components.

- **Users** of IM/IT, who will require foundational IM/IT skills including such things as the use of word processing, e-mail, on-line research tools, and decision-making tools. These 'users' include virtually every member of the DON.
- **Expert Users** of IM/IT require an increased knowledge of IM/IT during their tenure in a specific billet/position. Their required level of expertise is specifically associated with the job they need to accomplish. Examples of Navy and Marine Corps Enlisted Expert Users are shown in Exhibit 32. Samples of Civil Servant Expert User Occupational Series are shown in Exhibit 33.
- **Core IM/IT Professionals** are those military and civilians focused on IM/IT careers. They require specialized and concentrated competencies, reinforced with foundational and continual training and education. Examples of Core IM/IT Professionals in the Navy and Marine Corps and Civil Service are shown in Exhibits 34 and 35.

Navy Rating / Marine MOS	Description
OS, IS, AW, EW, AG	Communications and Intelligence specialists
STG & ET (not the primary NECs), AT, FC	Electronic Equipment Repairmen
AE, AM, GSE, EM, IC, EN, HT, DC	Electrical/Mechanical Equipment Repairmen
YN, PN, SK, DK, AZ, AK, CTA, LI, HM	Functional Support and Administration
QM, SM, BM	Seamanship Specialists
0612, 0613, 0614, 0619	Wiremen
0621, 0622, 0623, 0624, 0629	Radio Operators
0626, 0627, 0647, 0648	Communications Operators
2811, 2813, 2823, 2826, 2827, 2831, 28,32, 2833 2841, 2842, 2848, 2861, 2862, 2867, 2871, 2874, 2886, 2887, 2889,	Communications Maintenance
26xx, 46xx, 59xx, 63xx, 64xx,	Additional MOSs in staffing.

Exhibit 34. Navy and Marine Corps Enlisted Sample Expert Users

Occupational Series	Primary Occupational Title
0080	Security administrator
334	Computer Specialist
0340	Program Management
1550	Computer Scientist
0560	Budget Analyst
854	Computer Engineer
1102	Contracting Specialist
1515	Operations Research Analyst

Exhibit 35. Sample Civil Servant Expert User Occupational Series

Education and training is available for each level of IM/IT component, from ‘capstone’ training for executives to Class ‘A’ School for entry level users, to Class ‘C’ School equivalent for expert users in more technical jobs. The following categories of training are currently available.

Capstone Training. Capstone IM/IT training currently is provided in Flag rank and SES orientation classes as part of an executive overview of the issues and importance of IM/IT.

Professional Training. As specified by the Clinger-Cohen Act each major claimancy is required to have a CIO. A specific set of Federal competencies has been established for CIO's, and certification is available from the National Defense University . A description of the program and courses is available at the following website: www.ndu.edu.org/irmc. Eight of the following ten competencies are required for certification:

Acquisition
Policy
Strategic Planning
Process Improvement
Capital Planning and Investment
Performance and Results Based Management
Leadership
Technology Assessment
Security Assurance
Architectures and Infrastructure.

Eighty hours of IT training are required every two years to maintain certification.

Technical Training. For the military personnel Technical training Class 'A' / Class 'C' equivalent School is available. In addition, vendor/product training is an on-going requirement of the IT staff and should be included in personal development plans. Examples of the technical training required on an ongoing basis include Network management, Webpage development, Database Administration, Business Process Reengineering, Enterprise Resource Planning, Data standard and modeling, Security, and Information Assurance.

End-user Training. Class 'A' School, command training, plus vendor training. With command approval, IM/IT workforce members may complete academic courses to satisfy the continuous learning standards. Workforce members also are encouraged to explore work-related distributed-learning opportunities in advanced education. Opportunities to learn from experience may be made available to IM/IT workforce members as a normal part of their work assignments, or through rotational or developmental assignments specifically structured to provide broadening experiences.

The basic construct of the career path for civilian IM/IT workforce personnel, including skills and competencies, educational and experience opportunities for each IM/IT career field, is spelled out in the DON IM/IT Civilian Career Path Guide (CPG).

2.9. Outreach

The DON CIO, Service Data Administrators and the DMI PMO will develop an outreach strategy to ensure effective information flow and partnerships with DMI organizations and efforts within the DON as well as in other services, agencies, industry and foreign countries. The strategy will ensure the requirements of the DON are expressed at all levels and that proven processes and standards (international, national and DoD) are coordinated at the appropriate levels.

The strategy will encompass both the operational and acquisition communities, and it will maximize existing organizational involvements such as participation in the development of ISO standards and commercial working groups such a those concerned with XML specifications. It will recommend where MOA/MOU's with other agencies, e.g., DEA for Counternarcotics, should be developed to ensure interoperability. It also will develop industry incentives, e.g., preferred market access based upon certification and satisfaction of DMI requirements.

2.10. DMI Evaluation

In accordance with the requirements of the Clinger-Cohen Act, Measurements of Performance have been established for the DMI Strategic Goals and are listed below in Exhibit 36, DMI Measures of Performance. Measures of Performance and associated metrics should be established for all segments of the DMI Infrastructure.

DON DMI Strategic Goals	Measure of Performance
1. Provide a Data Management Interoperability Infrastructure that will Ensure Maritime Information Superiority	a. Navy and Marine Corps Implementing documents issued b. Service data administrators assigned c. Percent of Functional Data Managers (FDM) designated d. Adequate resources assigned to FDMs e. Percent of Authoritative Data Sources designated f. Percent of DMI efforts reviewed, and unified g. Percent of resource sponsor capital planning actions and budgets that include DMI
2. Reduce the Life Cycle Cost of Data Through Integration, Standards, and the Use of Authoritative Data Sources	a. Cost avoidance through re-use of standard data structures and reduced unique data interfaces b. Cost savings achieved through use of Authoritative Data Sources a. Cost savings achieved through database consolidation
3. Provide a DON DMI Repository and Tools to Support IT Assessments and Engineering	a. Metadata repository concept of operations defined and validated. b. Metadata repository specification defined and validated c. Standup of repository (Initial Operating Capability d. Percent of Year 2000 (Y2K) systems metadata registered in DMI Repository e. Progress in achieving correlation with national and international best practices f. Number of stored data elements g. Number of identified synonyms h. Number of identified homonyms
4. Provide a Data Architecture which addresses both Information Requirements and Data Capabilities	a. Percent of registered systems databases reconciled b. Percent completion of Functional Data Architectures c. Percent completion of Enterprise Data Architecture d. Degree of satisfaction of operational requirements by the current data architecture
5. Provide Processes and Metrics to Enable and Evaluate Data Management and Data Engineering	a. Number of processes and procedures developed b. Percentage of processes and procedures approved and implemented

Exhibit 36. DMI Measures of Performance

Metrics can be either developmental or on-going. Most of the following discussion pertains to on-going type metrics, however some mention must be made of developmental as they can provide some value as to how an organization is performing in the creation of systems, processes, etc. One unique characteristic of developmental MOEs is that they will not be repeatable once the system, process, etc., is in place and functioning normally. Nevertheless, they may be repeatable throughout the developmental process. Some examples are: developmental costs and performance against plans and schedules, DT&E type measures, percent of personnel hired for a system or process.

There are generally three types of metrics that can be either qualitative or quantitative:

- Process Metrics. (e.g., DMI Goal 5: processes for collecting and registering systems data and associated metadata, selecting and designating ADSs, etc.)
- Performance Metrics, (e.g., DMI Goals 3,4: number of systems registered, number of data elements reduced through reconciliation, percent completion of the Enterprise Architecture, etc.), and
- Program Metrics (e.g. DMI Goals 1,2: number of ADS assigned, percent of source sponsor budgets that include DMI, cost savings achieved through database consolidation, customer satisfaction, etc.

3. PLAN OF ACTION AND MILESTONES (POA&M)

3.1. Phase 0 – DMI Requirements and Concept Definition

Action	Responsibility	Reference	When
Issue SECNAVINST 5000.X, DMI	SECNAV	Section 1.2.2	Nov 2000
Issue DMI Strategic Plan	DON CIO, Navy CIO, Marine Corps CIO	Section 1.2.1	Nov 2000
Develop Business Plan	DON CIO	Section 3	Nov 2000
Issue DMI Implementation Planning Guide	DON CIO	Section 1.2.11	Nov 2000
Initiate DON DMIR (Pilot)	DON CIO	Sections 1.2.4, 2.4	Nov 2000
Designate PMO	DON CIO	Section 1.2.2.4	Dec 2000
Designate Service Data Administrators	CNO and CMC	Section 1.2.2.2	Dec 2000
Designate FDMs	CNO and CMC Resource Sponsors	Section 1.2.2.3	Dec 2000
Develop DMI Management Plan (charter)	PMO	Section 1.2.2.5	Jan 2001

3.2. Phase I – Implementation Planning and Portfolio Development

Action	Responsibility	Reference	When
Establish DMI Management Board	DON CIO	Section 1.2.2.5	Jan 2001
Identify DMI Priorities	DON CIO, Service DAs	Section 2.1.1	Jan 2001
Issue POM Guidance	SECNAV	Section 2.2	Jan 2001
Identify Bridge Funding	DON CIO, Service DAs	Section 2.2.1	Jan 2001
Integrate DMI into POMs	DON CIO, CNO, CMC	Section 2.2.2	Mar 2001
Establish measures of performance and metrics	DON CIO, PMO	Sections 1.2.10, 2.10	Mar 2001
Revise SECNAVINST 5000.2B (registration requirements)	SECNAV	Sections 1.2.3, 2.3	Mar 2001
Issue Joint DMI Instruction/Order	CNO and CMC	Sections 1.2.2, 2.1	Mar 2001
Issue Joint DMI	Service DAs	Sections 1.2.2, 2.1	Jun 2001

Action	Responsibility	Reference	When
Implementation Plan			
Commence FDM DMIR Implementation and DB Registration	DON CIO, PMO, FDMs	Section 2.4	Jun 2001
Establish high level enterprise data model	DON CIO, FDMs	Section 2.5.1	Jun 2001
Develop System Certification (8102) Plan	PMO	Section 1.2.7, 2.3.2, 2.3.3	Jun 2001
Issue System Certification (8102) Plan	DON CIO, Navy CIO, Marine Corps CIO	Section 1.2.7, 2.3.2, 2.3.3	Jul 2001
Develop System Data Interoperability Compliance Testing Criteria	PMO	Section 1.2.7, 2.3.2, 2.3.3, 2.7.1	Jun 2001
Issue System Data Interoperability Compliance Testing Criteria	DON CIO, RDA	Section 1.2.7, 2.3.2, 2.3.3, 2.7.1	Jul 2001
Develop Education and Training Plan	PMO, Service DAs	Sections 1.2.8, 2.8	Sep 2001
Develop Outreach Strategy	PMO, Service DAs	Sections 1.2.9, 2.9	Sep 2001
Develop Incentive Plan	PMO, Service DAs	Sections 1.2.9, 2.9	Sep 2001
Develop Logical Data Models (top-down)	FDMs	Sections 1.2.5, 2.5.3	Sep 2001
Designate ADS	FDMs	Sections 1.2.6, 2.6	Sep 2001
Perform System IT Registration for Certification	System Developers	Sections 1.2.4, 2.3.2, 2.5.2	Ongoing
Perform System Data Interoperability Compliance Testing	OPTEVFOR, NCTSI, Marine Corps	Sections 1.2.7, 2.3.3, 2.7.1	Ongoing
Collect feedback and measure effectiveness	DON CIO, Service DAs	Sections 1.2.10, 2.10	Ongoing
Provide lessons learned feedback to DMI community	DON CIO, Service DAs	Sections 1.2.8, 1.2.9, 2.8, 2.9	Ongoing
Coordinate DOD data standards proposals	CDAd, Service Das, FDMs	Section 2.5.5	Ongoing

3.3. Phase II – DON Functional Data Architectures (Established by each FDM)

Action	Responsibility	Reference	When
Begin training	PMO, Service DAs, FDMs	Sections 1.2.8, 2.8	Oct 2001
Register and Reconcile Operational Systems Metadata	FDMs	Sections 2.3.2, 2.5.2	Sep 2002
Develop Functional Data Models (bottom-up)	FDMs	Section 2.5.3	Sep 2002
Reconcile Functional Data Models (top-down, bottom-up within functional areas)	FDMs	Sections 2.5.3	Dec 2002
Develop standard data	FDMs	Section 2.5.5	Ongoing
Sustain DMI Infrastructure	DON CIO, Service DAs, Resource Sponsors	Sections 1.3, 2.1, 2.2	POM Cycle

3.4. Phase III – DON Enterprise Data Architecture (Modeled against the Defense Data Model)

Action	Responsibility	Reference	When
Reconcile Cross Functional Data Models	PMO, FDMs	Section 2.5.4	Jun 2003
Validate DON Data Architecture	DMI Management Board	Section 1.2.2.5, 2.1	Jul 2003
Sustain DMI Infrastructure	DON CIO, Service DAs, Resource Sponsors	Sections 1.3, 2.1, 2.2	POM Cycle

3.5. Action List by Role

The following tables provide a break out of responsibilities by organizational types.

3.5.1. DON CIO

Action	When	Reference
Issue DMI Strategic Plan	Nov 2000	Section 1.2.1
Develop Business Plan	Nov 2000	Section 3
Issue DMI Implementation Planning Guide	Nov 2000	Section 1.2.11
Initiate DON DMIR Pilot	Nov 2000	Sections 1.2.4, 2.4

Designate PMO	Dec 2000	Section 1.2.2.4
Establish DMI Management Board	Jan 2001	Section 1.2.2.4
Identify DMI Priorities	Jan 2001	Section 1.2.2.5
Identify Bridge Funding	Jan 2001	Section 2.2.1
Integrate DMI into POMs	Mar 2001	Section 2.2.2
Establish measures of performance and metrics	Mar 2001	Sections 1.2.10; 2.10
Commence FDM DMIR Implementation and DB registration	Jun 2001	Section 2.4
Establish high level data model	Jun 2001	Section 2.5.1
Issue System Certification (8102)	Jul 2001	Sections 1.2.7, 2.3.2, 2.3.3
Issue System Data Interoperability Compliance Testing Criteria	Jul 2001	Sections 1.2.7, 2.3.2, 2.3.3, 2.7.1
Collect feedback and measure effectiveness	Ongoing	Sections 1.2.10, 2.10
Provide lessons learned feedback to DMI community	Ongoing	Sections 1.2.8, 1.2.9, 2.8, 2.9
Sustain DMI Infrastructure	POM Cycle	Sections 1.3, 2.1, 2.2
Coordinate DoD data standards proposals	Ongoing	Section 2.5.5

3.5.2. Service Data Administrators Responsibilities

Action	**When**	**Reference**
Identify DMI priorities	Jan 2001	Section 2.1.1
Identify bridge funding	Jan 2001	Section 2.2.1
Issue Joint DMI Implementation Plan	Jun 2001	Sections 1.2.2, 2.1
Develop Education and Training Plan	Sep 2001	Sections 1.2.8, 2.8
Develop Outreach Strategy	Sep 2001	Sections 1.2.9, 2.9
Develop Incentive Plan	Sep 2001	Sections 1.2.9, 2.9
Collect feedback and measure effectiveness	Ongoing	Sections 1.2.9, 2.9
Provide lessons learned feedback to DMI community	Ongoing	Sections 1.28, 1.29, 2.8, 2.9
Coordinate DoD data standards proposals	Ongoing	Section 2.5.5
Begin training	Oct 2001	Sections 1.2.8, 2.8
Sustain DMI Infrastructure	POM Cycle	Sections 1.3, 2.1, 2.2

3.5.3. Program Management Office (PMO) Responsibilities

Action	When	Reference
Develop DMI Management Plan (charter)	Jan 2001	Section 1.2.2.5
Establish measures of performance and metrics	Mar 2001	Sections 1.2.10, 2.10
Commence FDM DMIR Implementation and DB registration	Jun 2001	Section 2.4
Develop System Certification (8102) Plan	Jun 2001	Sections 1.2.7, 2.3.2, 2.3.3
Develop System Data Interoperability Compliance Testing Criteria	Jun 2001	Sections 1.2.7, 2.3.3, 2.3.3, 2.7.1
Develop Education and Training Plan	Sep 2001	Sections 1.2.8, 2.8
Develop Outreach Strategy	Sep 2001	Sections 1.2.9, 2.9
Develop Incentive Plan	Sep 2001	Sections 1.2.9, 2.9
Begin training	Oct 2001	Sections 1.2.8, 2.8
Reconcile Cross Functional Data Models	Jun 2003	Sec 2.5.4

3.5.4. Functional Data Manager (FDM) Responsibilities

Action	When	Reference
Commence FDM DMIR implementation and system registration	Jun 2001	Section 1.1.4, Section 2.5.2
Register System Metadata	Sept 2001	Section 2.5.2
Reconcile System Metedata	Dec 2001	Section 2.5.3
Develop Logical Data Model for Functional Area	Mar 2002	Section 2.5.3
Develop Standard Data	Mar 2002	Section 2.5.5
Commence DoD Data Administration Process	Apr 2003	Section 2.5.5
Identify Authoritative Data Sources	Apr 2003	Section 1.2.6, Section 2.6
Reconcile Cross Functional Data Models	Dec 2002	Section 1.2.5, Section 2.5.3
Develop enterprise conceptual data model for DON	Mar 2003	Section 1.2.5, Section 2.5.1
Reconcile Functional Data Models to Operational Architecture Entity Relationship Models	Mar 2003	Section 1.2.5, Section 2.5.4
Provide Metrics to Customers	ongoing	Section 1.2.10, Section 2.10

Action	When	Reference
Manage Functional Database Configuration	ongoing	Section 2.4.2

3.5.5. System Developers/Program Managers Responsibilities

Action	When	Reference
Comply with data registration requirements in Section 8102	ongoing	Section 1.1.4, Section 2.3.2.2
Open DMIR account for new system by Milestone 0	ongoing	Section 2.3.2.1
Coordinate with FDM for reuse of existing data standards	ongoing	Section 1.2.4
Propose new candidate data standards to FDM	ongoing	Section 2.2.5
Complete registration of system by Milestone II	ongoing	Section 2.3.2.2
Provide Logical Data Model of system by Milestone II	ongoing	Section 2.3.2.2
Perform data compliance and conformance testing on new system	ongoing	Section 2.3.3

3.5.6. Resource Sponsor Responsibilities

Action	When	Reference
Designate FDMs	Dec 2000	Sections 1.2.2.3
Sustain DMI Intrastructure	POM Cycle	Sections 1.3, 2.1, 2.2

GLOSSARY

Assess. The act of estimating the value or condition of something. In the test community, this is typically a documentation review with little to no hands-on interface with the system.

Authoritative Data Source. Data products including databases that have been identified, described, and designated by appropriate DON Functional Data Managers, US Military Services and DOD Components for DOD support.

Capability. Any Information Technology and National Security Systems (Public Law 104-106) that enables or supports the production, use, or exchange of information, in any form electronically.

Capstone Requirements Document (CRD). A document that contains capabilities-based requirements that facilitates the development individual ORDs by providing a common framework and operational concept to guide their development. It is an oversight tool for overarching requirements for a system-of-systems or family-of-systems.

Compliance Testing. Compliance testing is usually performed in order to determine a numeric value, called compliance level, which is a measure of the degree to which a system or sub system conforms to the requirements of a standard.

Conceptual Data Model. A schema of the American National Standards Institute's (ANSI) Standards Planning and Requirements Committee's (SPARC) Three Schema Architecture, in which the structure of data is represented in a form independent of any physical storage or external presentation format.

Conformance Testing. Testing the extent a system or subsystem is conforming to or implementing a standard.

Data. A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. (FIPS Pub 11-3). Data are distinct pieces of information, usually formatted in a special way. All software is divided into two general categories: data and programs. Programs are collections of instructions for manipulating data.

Data Administration. The responsibility for definition, organization, supervision, and protection of data within an enterprise or organization. (NBS Special Publication 500-152)

Data Administrator (DA). A person or group that ensures the utility of data used within an organization by defining data policies and standards, planning for the efficient use of data, coordinating data structures among organizational components, performing logical data base designs, and defining data security procedures. (NBS Special Pub 500-152)

Data Architecture. A framework for organizing the interrelationships of data, (based on an organization's missions, functions, goals, objectives, and strategies), providing the basis for the incremental, ordered design and development of systems based on successively more detailed levels of data modeling. (DODD 8320.1)

Data Engineering. The discipline of decomposing information requirements into a system(s) data architecture. It includes database design, data standards, retrieval, authoritative data sources, distribution, and flow (interoperatiblity).

Data Interoperability. The ability to exchange and use data elements and values in any form between two or more systems or components (applications, segments, interfaces, etc.) such that they operate effectively and efficiently together.

Data Management. Data Management is a sub-set of Information Management. It deals with the creation, use, sharing, and disposition of data as a resource critical to the effective and efficient operation of functional activities. The structuring of functional processes to produce and monitor the use of data within functional activities, information systems, and computing and communications infrastructures. (DODD 8000.1 modified)

Data Management, for the purpose of this plan, adds the executive dimension to the data administration functions defined in DOD Directive 8320.1 of 26 Sep 91. The executive dimension assures DMI decisions reflect senior management goals and objectives. The operational dimension assures the data management infrastructure and functions are linked to current and future operational requirements.

Data Standard. A data element that has been through a formal analysis to reach agreement on its name, meaning, and characteristics, as well as its relationship to other standard data elements. Much like a common language, data standards enable processes and their supporting information systems to be integrated across functions, as well as within them, and improve the quality as well as the productivity of enterprise performance. (DEPSECDEF Memo of 13 Oct 1993, "Accelerated Implementation of Migration Systems, Data Standards, and Process Improvement)

Database. A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications; the data are stored so that they can be used by different programs without concern for the data structure or organization. A common approach is used to add new data and to modify and retrieve existing data. (FIPS Special Pub 11-3)

Database Segment. A standard method for packaging a physical database for incorporation into Shared Data Engineering (SHADE). Database segments are packaged like any other Common Operating Environment (COE) segment. (DII COE I&RTS, Version 4.0)

Data Interoperability. The ability to exchange and use data elements and values in any form between two or more systems or components (applications, segments, interfaces, etc.) such that they operate effectively and efficiently together.

DON Data Architecture. (DoD 8320.1-M-1 def) A framework for organizing the inter-relationships of DON data, (based on DON missions, functions, goals, objectives, and strategies), providing the basis for the incremental, ordered design an development of systems based on successively more detailed levels of data modeling.

Enterprise Conceptual Data Model. A conceptual model which results from the identification of super entities and the integration of the Enterprise Integrated Logical Data Model. The super entities are derived from the top-down analysis which includes the evaluation of MNS and ORDS.

Enterprise Integrated Logical Data Model. A logical model which is formed from the integration of the functional area logical models and maps to Enterprise Conceptual Model.

Family-of-Systems (FoS). A set or arrangement of independent systems that can be interconnected or related in various ways to provide different capabilities. The mix of systems can be tailored to provide desired capabilities dependent on the situation.

Functional Area. A functional area encompasses the scope (the boundaries) of a set of related functions and data for which an OSD Principal Staff Assistant or the Chairman of the Joint Chiefs of Staff has DoD-wide responsibility, authority, and accountability. A functional area (e.g., personnel) is composed of one or more functional activities (e.g., recruiting), each of which consists of one or more functional processes (e.g., interviews). Also known as a business area. (DoD 8320.1-M)

Functional Area Logical Data Model. A logical model which is formed from the integration of System Logical Data Models within a functional area and that maps to the Enterprise Integrated Logical Data Model.

Functional Data Manager. Organizations designated by the respective Resource and Program Sponsors to produce and control structuring of data within functional activities, information systems, and computing and communications infrastructures. Examples include: Naval Meteorology and Oceanography Command for meteorological and oceanographic data, Office of Naval Intelligence for characteristics and performance data of non-U.S. equipment and merchant ships, Naval Security Group for cryptologic information and data, DC/S Installations & Logistics (I&L) for Marine Corps logistics.

Horizontal Integration is the identification and consolidation of common data across functional areas.

Information. (1) Facts, data, or instructions in any medium or form. (2) The meaning that a human assigns to data by means of the known conventions used in their representation. (Joint Pub 1-02)

Information Assurance. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Also called IA. (Joint Pub 1-02)

Information Exchange Requirements (IER). The requirement for information to be passed between and among forces, organizations, or administrative structures concerning ongoing activities. Information exchange requirements identify who exchanges what information with whom, as well as, why the information is necessary and how that information will be used.

Information Management. The creation, use, sharing, and disposition of information as a resource critical to the effective and efficient operation of functional activities. The structuring of functional processes to produce and control the use of data and information within functional activities, information systems, and computing and communications infrastructures. (DODD 8000.1)

Information Superiority. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

Information Technology (IT). Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term "equipment" in this definition means equipment used by a Component directly, or used by a contractor under a contract with the Component, which requires the use of such equipment, or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "IT" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "IT" includes National Security Systems (NSSs). (Division E of Public Law 104-106, Section 5000(3)).

Infrastructure. The basic underlying resources used for data management including; data, data architecture and models, data management technology, metadata, processes, procedures and data standards. There are two components of the DON Data Management and Interoperability infrastructure:

- Management Component: DON CIO, ASN (RDA), Navy and Marine Corps Data Administrators, Board of Representatives, and the DMI Management Board.
- Engineering Component: DON Data Architecture which includes information requirements and models; and the DON DMI Repository which includes a systems catalog, systems database structures, data element definitions, transfer formats and standards, and data sources and users.

Interoperability is the ability of systems, units or forces to provide services to, and accept services from, other systems, units or forces, and to use the services so exchanged to enable them to operate effectively together (CJCS Pub 1-02).

Interoperability Assessment. The act or result of determining the contribution or disposition of an activity, product, or condition, based on an appraisal of the state of IT and NSS interoperability.

IT and NSS Interoperability. The exchange and use of information by IT and NSS in any form, electronically that enables effective operations for both warfighting and combat support areas both within the DoD and external activities, and synchronizes both materiel and non-materiel aspects.

Key Performance Parameter (KPP). Those capabilities or characteristics considered most essential for successful mission accomplishment. Failure to meet an ORD KPP threshold can be cause for the concept or system selection to be reevaluated or the program to be reassessed or terminated. Failure to meet a CRD KPP threshold can be cause for the FoS/SoS concept to be reassessed of the contributions of the individual systems to be reassessed. KPPs are validated by the JROC. ORD KPPs are included in the APB.

Knowledge Management. The strategies and processes to create, identify, capture, organize, and leverage vital skills, information, and knowledge to enable people to best accomplish the organizational missions (American Productivity and Quality Center).

Logical Data Model. A model of data that represents the inherent structure of that data and is independent of individual applications of the data and also of the software or hardware mechanisms which are employed in representing and using the data.

Metadata. Information describing the characteristics of data; data or information about data; descriptive information about an organization's data, data activities, systems, and holdings. (DOD 8320.1-M-1)

Milestones. Major decision points that separate the phases of an acquisition program.

Milestone Decision Authority (MDA). The individual designated in accordance with criteria established by the USD(AT&L) or by the ASD(C3I) for ITT and NSS acquisition programs, to approve entry of an acquisition program into the next phase

Military Department. Headed by a civilian Secretary appointed by the President and includes a Military Service (the Department of the Navy includes two Services).

Mission Need Statement (MNS). A formatted non-system-specific statement containing operational capability needs and written in broad operational terms. It describes required operational capabilities and constraints to be studied during the Concept Exploration and Definition Phase.

National Security System (NSS). Any telecommunications or information system operated by the United States Government, the function, operation, or use of which: (a) involves intelligence activities; (b) involves cryptologic activities related to national security; (c) involves command

and control of military forces; (d) involves equipment that is an integral part of a weapon or weapons system; or (e) subject to limitation below, is critical to the direct fulfillment of military or intelligence missions. Limitation—Item (e) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Network Centric Operations can be broadly described as deriving power from the rapid and robust networking of well-informed, geographically dispersed warfighters. They create overpowering tempo and a precise, agile style of maneuver warfare. Using effects-based operations, the aim is to sustain access and to decisively impact events ashore. Network Centric Operations focus on operational and tactical warfare, but they impact all levels of military activity from the tactical to the strategic. It is the emerging theory of war for the information age. (Naval Warfare Development Center Concept Paper dtd May 2000)

Operational Requirements. A system capability or characteristic required to accomplish approved mission needs. Operational (including supportability) requirements are typically performance parameters, but they may also be derived from cost and schedule. For each parameter, an objective and threshold value must also be established.

Operational Requirements Document (ORD). A formatted statement containing performance and related operational parameters for the proposed concept or system. Prepared by the user or users representative at each milestone beginning with Milestone 1.

Physical Data Model. A representation of the technologically independent requirements in a physical environment of hardware, software, and network configurations representing them in the constraints of an existing physical environment.

Program Manager. The organization responsible for the development and execution of a solution to a validated operational requirement. Also known as system developer.

Program Sponsor. The organization which validates operational requirements and supports development of solutions. Also known as resource sponsor.

Requirement. The need of an operational user, initially expressed in broad operational capability terms in the format of a MNS. It progressively evolves to system-specific performance requirements in the ORD.

Revolution in Business Affairs (RBA). RBA is a strategy that encompasses the following objectives: (1) sense of urgency to act among the top leaders, (2) broad leadership commitment and involvement, (3) engagement of leaders at several levels in initiatives across the Department, (4) early achievement of improvements, (5) a process that harnessed the best practices in strategic planning and business reengineering in the private sector, and (6) a systematic method to translate the best practices in business to DON activities.

Revolution in Military Affairs (RMA). RMA centers on developing the improved information and command and control capabilities needed to significantly enhance joint operations.

Super Entity. A high-level entity used in an enterprise-wide conceptual model to represent a broad category of data. These entities are presented without attributes. From the top-down approach, the super-entity is typically not implemented, but is used for sub-typing data entities in logical data models which can be implemented. From the bottom-up view, a super entity summarizes a category of entities.

System-of-Systems (SoS). A set or arrangement of systems that are related or interconnected to provide a given capability. The loss of any part of the system will degrade the performance or capabilities of the whole.

System Logical Data Model (SLDM. A logical model of a system under consideration by the DMI. The SLDM will be converted from the submitted form to a form that represents standard and developmental entities and attributes.

User. A user is a data customer.

View. (DoD 8320.1-M-1) A collection of entities and assigned attributes (domains) assembled for some purpose.

LIST OF ACRONYMS

ACAT	Acquisition Category
ACTD	Advanced Concept Technology Demonstration
ADS	Authoritative Data Sources
AOA	Analysis of Alternatives
ASD (C3I)	Assistant Secretary of Defense, Command, Control, Communications and Intelligence
ASN (RDA)	Assistant Secretary of the Navy, Research, Development and Acquisition
C4I	Command, Control, Communication, Computers and Intelligence
C4ISR	Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance
CADM	C4ISR Framework Architecture Data Model
CANs	Campus Area Networks
CBP	Commercial Business Practices
CDAd	Component Data Administrator
CDRL	Contract Data Requirement List
CHENG	Chief Engineer
CID	Combat Identification
CINCLANTFLT	Commander in Chief, Atlantic Fleet
CINCPAC	Commander in Chief, Pacific
CIO	Chief Information Office
CNO	Chief of Naval Operations
COE	Common Operating Environment
CONOPS	Concept of Operations
COTS	Commercial-off-the-Shelf
CPG	Civilian Career Path Guide
CRD	Capstone Requirements Document
DBMS	Database Management System
DDDS	Defense Data Dictionary System
DDL	Data Definition Language
DIA	Defense Intelligence Agency
DID	Data Item Description
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DMI	Data Management and Interoperability
DMIR	Data Management and Interoperability Repository
DOD	Department of Defense
DODDAd	Department of Defense Data Administrator
DON	Department of the Navy
DRWG	Data Requirements Working Group

EA	Executive Agent
EDI	Electronic Data Interchange
EPL	Electronic Parameters List
ERP	Enterprise Resource Planning
EW	Electronic Warfare
FDAd	Functional Data Administrator
FDM	Functional Data Managers
FIWC	Fleet Information Warfare Center
FoS	Family of System
FYDP	Future Year’s Defense Program
GIG	Global Information Grid
GMRA	Government Management Reform Act
GNIE	Global Networked Information Enterprise
G&P	Guidance and Policy
G&PM	Guidance and Policy Memoranda
GPRA	Government Performance and Results Act
IA	Information Assurance
IDEFIX	Integrated Computer Aided manufacturing (ICAM) Definition Information Model
IDP	Individual Development Plans
IEs	Information Elements
IERs	Information Exchange Requirements
IM/IT	Information Management/Information Technology
IPT	
I&RTS	Integration and Runtime Specification
ISO	International Standards Group
ITA	Information Technology Architecture
ITIA	Information Technology Infrastructure Architecture
ITSG	Information Technology Standards Guidance
JT&Es	Joint Test and Evaluations
KM	Knowledge Management
KPP	Key Performance Parameters
LANs	Local Area Networks
LISI	Levels of Information System Interoperability
MAISs	Major Automated Information Systems
MANs	Metropolitan Area Networks
MDAPs	Major Defense Acquisition Programs
METOC	Meteorology and Oceanographic Command
MFP	Major Force Programs

MIDB	Modernized Intelligence Database
MNS	Mission Need Statement
MOA	Memorandum of Agreement
MOEs	Measures of Effectiveness
MOPs	Measures of Performance
MOU's	Memorandum of Understanding
NATO	North Atlantic Treaty Organization
NAVSEA	Naval Sea Systems Command
NIPRNET	Navy Internet Protocol Router Network
NMCI	Navy/Marine Corps Intranet
NSA	National Security Agency
NSS	National Security System
OA	Operational Architecture
OMB	Office of Management and Budget
OPNAVINST	Chief of Naval Operations Instruction
ORDs	Operational Requirement Documents
OSD	Office of the Secretary of Defense
OS	Operating System
PDM	Program Decision Memorandum
PEO	Program Executive Officers
PM	Program Manager
PMO	Program Manager Office
POA&M	Plan of Action and Milestones
POM	Program Objective Memorandum
PPBS	Planning, Programming and Budgeting System
PR	Program Review
PSA	Principal Staff Assistants
RAPADS	Radar Parameters Data Set
RBA EXCOM	Revolution in Business Affairs Executive Committee
ROI	Return-On-Investment
SECNAVINST	Secretary of the Navy Instruction
SDAd	Service Data Administrators
SHADE	Shared Data Engineering
SIAP	Single Integrated Air Picture
SIPRNET	Secure Internet Protocol Router Network
SoS	System of System
SOW	Statement of Work
TEMPs	Test and Evaluation Master Plans
USD (AT&L)	Under Secretary of Defense, Acquisition, Technology and Logistics

WANs	Wide Area Networks
WBS	Work Breakdown Structure
XML	eXtensible Markup Language
Y2K	Year 2000

Appendix A
Statement of Work DMI Trigger Clause

For any Acquisition of an Information Technology System, as defined by Public Law 104-____ (Clinger-Cohen), Public Law 105-261 Section 331 (Strom Thurmond), and FY-2000 Defense Authorization Act Section 8121, that requires an application data store or which defines an application data requirement, the following SOW clause shall apply:

"The contractor shall

(1) to the extent possible reuse metadata from the existing functional area metadata baseline;
(2) only when metadata from the functional area metadata baseline cannot be reused or modified shall new candidate system metadata be proposed.
(3) Candidate system metadata subsequently defined using these guidelines shall be registered in the DON DMIR IAW CDRL #________ in the format defined in Data Item Description #__________.

Appendix B
Sample Data Item Description (DID)

DATA ITEM DESCRIPTION	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. TITLE System Metadata Registration Requirements Data	2. IDENTIFICATION NUMBER

3. DESCRIPTION / PURPOSE

3.1 The System Data Requirements Registration is used to capture the scope and content of a system's metadata (metadata is defined as data about data) to be used by an information processing system that will require data/database support throughout its life-cycle.

4. APPROVAL DATE *DRAFT*	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR) N – Dept of the Navy Chief Information Officer	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE

7. APPLICATION / INTERRELATIONSHIP

7.1 The System Metadata Registration Requirements Data will be used to develop data standards for reuse in peer and follow-on information processing systems.

7.2 Information to be acquired through these data will include data element names, data element definitions, data element domains, data element valid values, data element ranges, data element precision, and (continued on page 2)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER

10. PREPARATION INSTRUCTIONS

10.1 **General Instructions**

a. **Automated Techniques.** Use of automated techniques is encouraged. The term "document" in this DID means a collection of data regardless of its medium. The recommended CASE tool for data collection, formatting, and delivery, is the government owned Data Analysis and Reconciliation Tool (DART). DART is available at no cost from the Dept of the Navy, Office of the Chief Information **Officer.**

b. **Title Page or Identifier.** The document shall include a title page containing, as applicable, document number; volume number; version/revision indicator; security marking or other restrictions on the handling of the document; date; document title; name abbreviation, and any other identifier for the system, subsystem, or item to which the document applies; contract number; CDRL item number; organization for which the document has been prepared; name and address of the preparing organization; and distribution statement. For data in a database or other alternative form, this information shall be included on external and internal labels or by equivalent identification methods.

(continued on page 2)

11. DISTRIBUTION STATEMENT

DATA ITEM DESCRIPTION	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. TITLE System Metadata Registration Requirements Data	2. IDENTIFICATION NUMBER

3. DESCRIPTION / PURPOSE

4. APPROVAL DATE *DRAFT*	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR) N - Dept of the Navy Chief Information Officer	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE

7. APPLICATION / INTERRELATIONSHIP

7.2 (continued from page 1) and other metrics.

7.3 This DID is used when the developer is tasked by the contract to define and record the design of one of more databases.

7.4 Wherever possible the data requirements of a system will be satisfied by accessing it from an existing system consistent with established DoD Policy for data re-use. The DMIR contains information(continued on page 3)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER

10. PREPARATION INSTRUCTIONS

a. **Response to Tailoring Instructions.** If a paragraph is tailored out of this DID, the resulting document shall contain the corresponding paragraph number and title, followed by “This paragraph has been tailored out.”

b. **Content Requirements.** Content requirements begin on the following page. The numbers shown designate the paragraph numbers to be used for each data element metadata description used in the document. The first paragraph is understood to have the prefix “10.2” within this DID. For example, the first paragraph numbered 1.1 is understood to be paragraph 10.2.1.1 within this DID. Paragraph numbering after 10.2 will continue sequentially until all data elements used within the database have been documented.

(continued on page 3)

11. DISTRIBUTION STATEMENT

Previous editions are obsolete

DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. TITLE

System Metadata Registration Requirements Data

2. IDENTIFICATION NUMBER

3. DESCRIPTION / PURPOSE

4. APPROVAL DATE
DRAFT

5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)
N - Dept of the Navy Chief Information Officer

6a. DTIC APPLICABLE

6b. GIDEP APPLICABLE

7. APPLICATION / INTERRELATIONSHIP

(continued from page 2)

7.4 (continued) on the available interfaces to existing systems. Where this method obtains re-use of this existing data source will be registered in accordance with ____________________.

7.5 Where data from an existing system cannot be used but the metadata about it does exist in the DMIR, the data will be implemented in

(continued on page 4)

8. APPROVAL LIMITATION

9a. APPLICABLE FORMS

9b. AMSC NUMBER

10. PREPARATION INSTRUCTIONS

(Continued from page 2)

1. **Data Attribute.**

1.1 **Data Attribute Name.** The label of an attribute, comprised of a minimum of an entity and generic element; may contain property modifier(s) providing additional descriptions; may utilize generic data; must be a noun or noun phrase and accurately reflect the characteristics (metadata) of the attribute, especially domains.

1.2 **Data Attribute Abbreviated Name.** A short abbreviated name representing a specific data element. An access name is used to reference a data element in a database and must conform to the syntactical requirements of the database management system (DBMS) or programming language of the application in which a data element is used. The maximum length for an access name is 18 characters.

1.3 **Data Attribute Definition.** The narrative describing the meaning of a standard data element.

(continued on page 4)

11. DISTRIBUTION STATEMENT

Previous editions are obsolete

DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. TITLE
System Metadata Registration Requirements Data

2. IDENTIFICATION NUMBER

3. DESCRIPTION / PURPOSE

4. APPROVAL DATE
DRAFT

5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)
N – Dept of the Navy Chief Information Officer

6a. DTIC APPLICABLE

6b. GIDEP APPLICABLE

7. APPLICATION / INTERRELATIONSHIP

(continued from page 3)

7.5 (continued) the registering system but in accordance with the metadata about it, already in the DMIR. In this case a reason will be provided for not using the data in the existing system. The reuse of this metadata will be registered in accordance with ________________.

7.6 Only when a data requirement cannot be met using metadata already

(continued on page 5)

8. APPROVAL LIMITATION

9a. APPLICABLE FORMS

9b. AMSC NUMBER

10. PREPARATION INSTRUCTIONS

(continued from page 3)

1.1 **Data Attribute Data Type.** The name of the way domain values are stored in a database. The generic data elements with class words having a data type of “integer” will be modified with a comment (comment text field) as follows: data element using the data type “integer” should fit into a 32 bit representation. The high range value of a signed interger is limited to “2.1 billion” (in the range –2^{31} to 2^{31} –1); data requirements of greater values should use the data types “floating point” and “fixed point.”

1.2 **Data Attribute Column Width.** The field length of the data; it should be large enough to accommodate all requirements, yet precise enough to allow for accuracy.

1.3 **Data Attribute Precision.** The integers that indicate the quantity of numeric digits allowed to the right of the decimal point in a quantitative fixed point domain value.

(continued on page 5)

11. DISTRIBUTION STATEMENT

DATA ITEM DESCRIPTION	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. TITLE System Metadata Registration Requirements Data	2. IDENTIFICATION NUMBER

3. DESCRIPTION / PURPOSE

4. APPROVAL DATE *DRAFT*	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR) N - Dept of the Navy Chief Information Officer	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE

7. APPLICATION / INTERRELATIONSHIP

(continued from page 4)

7.6 (continued) in the DMIR will a new metadata ?primitive? be registered in accordance with _____________________. If a reasonable person might suspect the usability of existing metadata, a justification for not doing so will be provided.

Under no circumstances will a data requirement be satisfied by the

(continued on page 6)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER

10. PREPARATION INSTRUCTIONS

(continued from page 4)

1.1 **Data Attribute Unit of Measure.** The word(s) that express the term in which the dimension, quantity, or capacity of an object can be stated.

1.2 **Data Attribute Domain High.** A string of up to 20 integers that indicates the largest allowed domain value when a data element's domain is expressed as a range of acceptable values.

1.3 **Data Attribute Domain Low.** A string of up to 20 integers that indicates the smallest allowed domain value when a data element's domain value when a data element's domain is expressed as a range of acceptable values.

1.4 **Data Attribute Classification Code.** A classification assigned to the data element domain value identifiers stored in some physical media to show the level of protection required to prevent their disclosure.

1.5 **Data Attribute Revision Date.** The amendment date of a data

(continued on page 6)

11. DISTRIBUTION STATEMENT

DATA ITEM DESCRIPTION	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. TITLE System Metadata Registration Requirements Data	2. IDENTIFICATION NUMBER

3. DESCRIPTION / PURPOSE

4. APPROVAL DATE *DRAFT*	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR) N - Dept of the Navy Chief Information Officer	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE

7. APPLICATION / INTERRELATIONSHIP

(continued from page 5)

7.7 (continued) system being developed or maintained without the fact being registered in some way within the DMIR.

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER

10. PREPARATION INSTRUCTIONS

(continued from page 5)

1.11 (continued) attribute.

1.12 **Data Attribute Timeliness Code.** A description of the frequency of updates to the domain, this information will inform implementers and/or database administrators when to refresh their tables.

NOTE: REMAINING ATTRIBUTES FROM THE DMIR REGISTRATION TEMPLATE WILL BE DEFINED.

11. DISTRIBUTION STATEMENT

DD Form 1664, AUG 96 (EG) *Previous editions are obsolete* Page 6 of 6 Pages

Appendix C
DMI Repository System Registration Forms

ENTITY	ATTRIBUTE	DATA TYPE	LENGTH	DEFINITION
System	System Name	CHAR	240	The name of a system.
	System Acronym Text	CHAR	50	The abbreviation of the name of a specific system.
	System Description Text	CHAR	2000	The text that briefly characterizes a specific system.
	System Classification Code	CHAR	2	The code that denotes a classification category of a specific system. *
	System Version Name	CHAR	240	The name that identifies a specific form of a specific system.
	System 8121/8102 Compliance Status Code **	CHAR	2	System compliance to 8121/8102. *
	System Mission Critical Code **	CHAR	3	System mission critical code name
	System Type Code **	CHAR	2	System type code name. **
System Configuration	Sys Configuration Name	CHAR	240	The name of a system configuration.
	Sys Configuration Description Text	CHAR	2000	The text that briefly characterizes a specific system configuration.
	Sys Configuration Classification Code	CHAR	2	The code that denotes a classification category of a specific system configuration. *
Organization	Organization Name Text	CHAR	250	The text of an organization name.
	Organization Description Text	CHAR	999	The text describing an organization.
	Organization Unit Identification Code	CHAR	20	A code that represents the unit identification of an organization.
Point of Contact	POC First Name Text	CHAR	25	The given name for a specific point of contact.
	POC Last Name Text	CHAR	25	The family name for a specific point of contact.
	POC Address Line1 Text	CHAR	99	POC street/office address.
	POC Address Line2 Text	CHAR	99	POC additional street/office address information.
	POC City Text	CHAR	99	POC city/place address.
	POC State Code	CHAR	2	POC state name.
	POC ZIP Code Text	CHAR	15	POC ZIP codes.
	POC Country Name Text	CHAR	25	POC Country name.
	POC Commercial Phone Number Text	CHAR	20	Phone number for POC.
	POC FAX Number Text	CHAR	20	The FAX number for the POC.
	POC Unclassified EMail Text	CHAR	40	The unclassified e-mail address for the POC.
Program Element	Program Element Name	CHAR	240	The name of a program element associated with system.
Mission Area	Mission Area Name	CHAR	50	The name of a mission area. *
Functional Area	Functional Area Name	CHAR	60	The name of a functional area. *

* Select from a picklist of valid values.

** Applies to those systems that have registered in accordance with DoD appropriations acts.

ENTITY	ATTRIBUTE	DATA TYPE	LENGTH	DEFINITION
INFORMATION ASSET	INFORMATION ASSET Name	CHAR	240	The name of an information-asset.
	INFORMATION ASSET Acronym Text	CHAR	60	The text that describes the initial characters of the name of an information-asset.
	INFORMATION ASSET Definition Text	CHAR	2000	The text that defines an information-asset.
	INFORMATION ASSET Type Code	CHAR	2	The code that represents a kind of information-asset. *
DATA-ENTITY	DATA-ENTITY NAME	CHAR	240	The name of a data-entity.
	DATA-ENTITY SHORT NAME	CHAR	60	The abbreviated name of a data-entity.
	DATA-ENTITY DEFINITION	CHAR	2000	The text that describes a data-entity.
	DATA-ENTITY REVISION DATE	DATE		The amendment date of a data-entity.
DATA-ATTRIBUTE	DATA-ATTRIBUTE NAME	CHAR	250	The name of a data-attribute.
	DATA-ATTRIBUTE ABBREVIATED NAME	CHAR	30	The name of the shortened form of a data-attribute.
	DATA-ATTRIBUTE DEFINITION	CHAR	2000	The text that defines a data-attribute.
	DATA-ATTRIBUTE DATA TYPE CODE	CHAR	16	The code that represents a kind of data type identifier of a data-attribute.
	DATA-ATTRIBUTE COLUMN WIDTH	INTEGER		The quantity of column width of a data-attribute.
	DATA-ATTRIBUTE UNIT OF MEASURE	CHAR	30	The code that represents the unit of measure for a data-attribute.
	DATA-ATTRIBUTE DOMAIN HIGH	CHAR	25	The quantity the represents the domain high value of a data-attribute.
	DATA-ATTRIBUTE DOMAIN LOW	CHAR	25	The quantity the represents the domain low value of a data-attribute.
	DATA-ATTRIBUTE REVISION DATE	DATE		The amendment date of a data-attribute.
	DATA-ATTRIBUTE TIMELINESS CODE	CHAR	3	The code that represents the frequency update of a data-attribute.
	DATA-ATTRIBUTE PRECISION	INTEGER		The quantity of precision that represents a data-attribute
DATA-DOMAIN	DATA-DOMAIN-VALUE NAME	CHAR	60	The name of a data-domain-value.
	DATA-DOMAIN-VALUE DESCRIPTION TEXT	CHAR	120	The text that describes a data-domain-value.
	DATA-DOMAIN CONSTRUCTION TYPE CODE	CHAR	1	The code that represents a kind of construct of a data-domain.
	DATA-DOMAIN-LIST SOURCE LIST TEXT	CHAR	80	The text of the origin of a listing in a data-domain-list.
INTERNAL-DATA-MODEL	INTERNAL-DATA-MODEL TECHNOLOGY NAME	CHAR	100	The name of the technical aspects of an internal-data-model.

* Select from a picklist of valid values.